ONEOS V4.3R4

ONEOS V5.1R3

VOICE OVER IP USER GUIDE

(EDITION 10)

OneAccess Networks
Pentagone Plaza
381, Avenue du Général de Gaulle
92140 Clamart
FRANCE

The law of 11 March 1957, paragraphs 2 and 3 of article 41, only authorizes, firstly, "copies and reproductions strictly reserved for use by copyists and not for general use and, secondly, analyses and short quotations for the purpose of example and illustration. Therefore, "any representation or reproduction, entire or partial, made without the consent of the author or his representatives is illegal" (paragraph 1 of article 40).

Any such representation or reproduction, made in any manner whatsoever, would therefore constitute an infringement of the law as sanctioned by articles 425 and in accordance with the penal code.

Information contained in this document is subject to change without prior notice and does not constitute any form of obligation on the part of OneAccess.

OneAccess and the distributors can in no case be held responsible for direct or indirect damage of any kind incurred as a result of any error in the software or guide.

Every care has been taken to ensure the exactitude of information in this manual. If however you discover an error, please contact OneAccess After Sales Service division.

Tenth edition: July 2011

1 INTRODUCTION

This edition of the OneOS Voice Manual corresponds to the V4.3R4 and V5.1R3 software releases of OneOS. It is also available for all previous software releases of OneOS according to the feature matrix described hereafter.

The OneOS software developed for use with the ONE product range offers an extensive range of features designed to provide a complete & highly powerful range of multi-service access routers:

- Full IP router with NAPT, Security, and Quality of Service management
- Support of voice for analog and ISDN S0/T0 terminals using Voice over IP and Voice over ATM
- Interworking of data protocols (FR, X.25, PAD, XOT, X.31)
- Advanced management tools based on CLI (Command Line Interface), SNMP, FTP/TFTP

This document is the OneOS user guide for voice over IP-related functions of the OneOS-based range products that are voice enabled.

Seven other user guides and two global indexes are available:

- OneOS – Admin User Guide
- OneOS – Bridging & LAN User Guide
- OneOS – Basic IP User Guide
- OneOS – Advanced IP User Guide
- OneOS – WAN User Guide
- OneOS – VoATM & CES User Guide
- OneOS – IBC User Guide
- Index of OneOS User Guides (global table of contents)
- Index of CLI of OneOS User Guides (global list of CLI commands)

1.1 FEATURE MATRIX

The following table is a resource providing edition by edition the released features. The table was done as of the release V3.5R2E3. For simplification, the indicated software release shows the presence of a feature in a given software release. It should be noted that most features were available in earlier versions.

Main Function	Feature	Present at least in:
VoIP (SIP/H.323 common functions)	RAI support	V3.5R2E3
	Intrusive mode (connection enabled when local voice ports are up)	V3.5R2E3
	Support of en-bloc and overlap dialing	V3.5R2E3
	Direct call (automatic call after off-hook)	V3.5R2E3
	Fully configurable ringing tones	V3.5R2E3
	FSK/DTMF caller-id presentation on POTS terminal interface	V3.5R2E3
	Voice call routing	V3.5R2E3
	- between local ports	V3.5R2E3
	- backup routing	V3.5R2E3
	- pre- and post-routing calling/called number translation (translation based on wildcards)	V3.5R2E3
	- call routing to a group of interfaces (call distribution based on priority and round robin)	V3.5R2E3
	- call routing to a group of interfaces (call distribution based on priority and least load port)	V4.2R5E15
	Call hunting	V3.5R2E3
	Codec: G.711, G.729A, clear channel mode (unrestricted data)	V3.5R2E3
	ISDN terminal synchronization from received SNTP clock	V3.5R2E3
	RTP bandwidth limitation	V3.5R2E3
	G3 and super G3 fax support: fax pass-through and fax relay (T.38)	V3.5R2E3
	Echo cancellation disabling when detecting fax/modem	V3.5R2E3
	Configurable ringing tones for various countries	V3.5R2E3
	Clock synchronization: RTP, DSL, free-run, slave	V3.5R2E3
	Configurable jitter	V3.5R2E3
	Silence detection / comfort noise	V3.5R2E3
	RTP extended statistics (loss, jitter, voice quality diagnostics)	V3.5R2E3
	Force ISDN layer-2 activity	V3.5R2E3
	Permanent layer-2 improvement; permanent layer-1	V4.2R5E2
	ISDN channel specialization	V3.5R2E3
	T.38 ECM	V3.7R3E1
	International numbering plan management	V4.2R5E2
	SuperG3 to G3 FAX fallback	V3.7R11E14
	Call Admission and Control	V3.7R11E14
	Services on ISDN ports	V3.7R11E14
	RTP adaptive clock synchronization	V3.7R11E14
	Compatibility with external hosted NAT traversal	V3.7R11E14

Main Function	Feature	Present at least in:
	Emergency calls	V3.7R11E14
MOS Scoring	MOS-LQ / MOS-CQ calculation	V4.2R5E2
	R factor display	V4.2R5E2
SIP (additional functions)	Registration	V3.6R5E3
	WWW authentication	V3.6R5E3
	OPTIONS	V3.6R5E3
	Voice routing and call backup routing	V3.6R5E3
	DTMF in-band (RFC 2833 method)	V3.6R5E3
	DTMF out-band (SIP INFO method)	V3.6R5E3
	Separate configuration of SIP user/password, SIP ID	V3.6R5E3
	Authentication in INVITE	V3.6R5E3
	Ability to change URI format in Contact and From fields	V3.6R5E3
	CLIP / CLIR / COLP / COLR support for ISDN	V3.6R5E3
	SIP Proxy with NAT ALG	V3.7R3E1
	SIP request timeout configurable	V3.7R10E3
	Internally managed FXS services (hold, retrieve, brokering, call transfer, 3-way conference)	V3.7R10E3
	SIP call routing based on Request URI, P-Called-Party-ID and To fields	V3.7R10E3
	External conference bridge support	V3.7R10E3
	External voicemail	V3.7R10E3
	Configuration of request method timeout	V3.7R10E3
	Allow discard of 3XX message	V3.7R10E3
	Services on FXS port (intelligent mode)	V3.7R11E14
	HLC & LLC insertion	V3.7R11E14
	MWI service	V3.7R11E14
	FXS Line Voltage Drop	V3.7R11E14
	Dynamic payload type	V3.7R11E14
	AOC TISPAN	V.4.2R6E5
	SIP for E1 R2 interface	V4.2R7E2
H.323 (additional functions)	H.323 V4	V3.5R2E3
	Fast connect	V3.5R2E3
	AOC (CS2K specific feature)	V3.5R2E3
	DTMF in H.245 and DTMF in-band (RFC 2833)	V3.5R2E3
	TCS null support (reset of H.323 media channel)	V3.5R2E3
	Gatekeeper discovery, alternate gatekeeper support	V3.5R2E3
	CLIP / CLIR / COLP / COLR support for ISDN	V3.5R2E3
MGCP	MGCP for FXS interfaces	V3.6R4E5
	Fax detection, pass-through (G.711 codec without echo cancellation switching) or relay (T.38)	V3.6R4E5
	Modem detection and pass-through	V3.6R4E5
	DTMF in-band (RFC 2833) and out-of-band (MGCP DTMF package)	V3.6R4E5

1.2 TABLE OF CONTENTS

1 INTRODUCTION....1.1-3

1.1 Feature Matrix....1.1-4
1.2 Table of Contents....1.2-6

2 VOICE OVER IP....1.2-11

2.1 Introduction to SIP & H.323....2.1-11
2.2 SIP and H.323 Overall Architecture....2.2-11

3 H.323 PACKET-BASED MULTIMEDIA COMMUNICATIONS SYSTEMS....2.2-13

3.1 H.323 Protocol Overview....3.1-13
3.1.1 H.323 Signaling Processing....3.1-13
3.1.2 Use of a Gatekeeper....3.1-13
3.1.2.1 Resource Management (RAI)....3.1-14
3.1.2.2 Intrusive mode....3.1-14
3.1.3 Application Cases....3.1-14
3.2 H.323 – ISDN Signaling Gateway....3.2-15
3.2.1 Dialing....3.2-15
3.2.2 Ringback tones and announcements....3.2-16
3.2.3 Disconnection....3.2-16
3.2.4 Advice of charge....3.2-17
3.2.5 Complementary Services....3.2-17
3.3 H.323 Analog Port Signaling....3.3-18
3.3.1 Dialing....3.3-18
3.3.2 Tones & Announcements....3.3-18
3.3.3 Ringing....3.3-18
3.3.4 Caller Identification....3.3-18
3.3.5 H.245 Terminal Capabilities....3.3-18
3.3.6 Advice of charge....3.3-18
3.3.7 Line Power Drop....3.3-18
3.4 H.323 FXO Port Signaling....3.4-19
3.4.1 Outgoing Call....3.4-19
3.4.2 Incoming Call....3.4-19

4 SIP SESSION INITIATION PROTOCOL....3.4-20

4.1 SIP Protocol Overview....4.1-20
4.1.1 SIP Signaling Processing....4.1-20
4.1.2 Dialog with SIP-Proxy....4.1-20
4.1.3 Dialog via Outbound Proxy....4.1-20
4.1.4 Voice Path Establishment....4.1-21
4.1.5 "From", "To" and "Contact" fields configuration....4.1-21
4.1.6 Mapping of Release Causes....4.1-21
4.2 SIP Complementary services....4.2-25
4.2.1 SIP/FXS interworking....4.2-25
4.2.2 SIP/ISDN interworking....4.2-25
4.2.3 CLIP/CLIR Complementary Services....4.2-25
4.2.3.1 CLIP Complementary Service....4.2-25
4.2.3.2 CLIR Complementary Service....4.2-26
4.2.3.3 CLIP/CLIR interworking process in SIP to ISDN call....4.2-26
4.2.3.4 CLIP/CLIR interworking process in ISDN to SIP call....4.2-26
4.2.4 COLP/COLR Complementary Services....4.2-26
4.2.4.1 COLP Complementary Service....4.2-26
4.2.4.2 COLR Complementary Service....4.2-27
4.2.4.3 COLP/COLR interworking process in SIP to ISDN call....4.2-27
4.2.4.4 COLP/COLR interworking process in ISDN to SIP call....4.2-27
4.2.5 UUS Complementary Service....4.2-27
4.2.5.1 UUS ISDN service....4.2-27

4.2.5.2 UUS interworking process 4.2-27

5 VOIP CALL ROUTING AND VOICE PROCESSING 4.2-28

5.1 VoIP Call Routing 5.1-28
5.1.1 Incoming Call Routing 5.1-28
5.1.2 Call distribution 5.1-28
5.1.3 Call Hunting 5.1-29
5.1.4 Backup Call Routing 5.1-29
5.1.5 Number Translation 5.1-29
5.1.5.1 Calling Number Translation on Local Ports 5.1-29
5.1.5.2 Calling & Called Number Translation by Using the Routing Table 5.1-29
5.1.6 Bearer Capability processing 5.1-29
5.1.7 Tones and Announcements 5.1-30
5.1.8 Numbering plan management and Routing process 5.1-30
5.1.9 Call-Triggered Reboot 5.1-30
5.1.10 Date & Time 5.1-30
5.1.11 Number Portability 5.1-30
5.2 VoIP Voice Processing 5.2-31
5.2.1 Hosted Nat Traversal 5.2-31
5.2.2 Bandwidth Limitation 5.2-31
5.2.3 Emergency calls 5.2-32
5.2.4 Group 3 FAX Processing 5.2-32
5.2.5 Modem Processing 5.2-33
5.2.6 Echo Processing and Pass-through modes 5.2-33
5.2.7 DTMF Processing 5.2-33
5.2.8 MOS scoring 5.2-33

6 VOIP CONFIGURATION 5.2-35

6.1 Introduction to VoIP Configuration 6.1-35
6.1.1 Configuration Items 6.1-35
6.1.2 Configuration Management 6.1-36
6.2 VoIP: Physical Voice Ports Configuration 6.2-37
6.2.1 Common parameters 6.2-37
6.2.1.1 Parameters for Echo Cancellation 6.2-37
6.2.1.2 Parameters for Gain control 6.2-38
6.2.1.3 Parameters for Synchronization 6.2-38
6.2.1.4 Parameters for Tones 6.2-39
6.2.1.5 Parameters for Dialing 6.2-40
6.2.1.6 Parameters for Advice of Charge 6.2-40
6.2.1.7 Miscellaneous Parameters 6.2-41
6.2.2 ISDN ports specific parameters 6.2-41
6.2.2.1 Parameters for Power Source One (ISDN ports only) 6.2-41
6.2.2.2 Parameters for Tones (ISDN ports only) 6.2-41
6.2.2.3 Parameters for User-to-User Service (ISDN ports only) 6.2-42
6.2.2.4 Parameters for Call Forwarding Service (ISDN ports only) 6.2-42
6.2.3 Analog ports specific parameters 6.2-43
6.2.3.1 Parameters for ringing (analog ports only) 6.2-43
6.2.3.2 Parameters for Loop State management (analog ports only) 6.2-44
6.2.3.3 Parameters for Country-specific Characteristics (analog ports only) 6.2-44
6.2.3.4 Parameters for FXS Line Power Drop (analog ports only) 6.2-45
6.2.3.5 Parameters for Analog MWI (analog ports only) 6.2-45
6.2.3.6 Parameters for Analog CLIP (analog ports only) 6.2-46
6.2.3.7 Parameter for Reverse Ringback Tone (analog ports only) 6.2-46
6.2.3.8 Parameter for Call-waiting duration (analog ports only) 6.2-46
6.2.4 FXS Supplementary Services Parameters 6.2-47
6.2.4.1 Configuring FXS Voice Features 6.2-47
6.2.4.2 Using FXS Voice Features 6.2-49
6.2.4.2.1 Call Waiting 6.2-49
6.2.4.2.2 Second Call 6.2-49
6.2.4.2.3 Releasing Second Call 6.2-49
6.2.4.2.4 Brokering 6.2-50
6.2.4.2.5 Attended Call Transfer 6.2-50
6.2.4.2.6 Three-Way Conference 6.2-51
6.2.5 Obsolete Parameters 6.2-51
6.3 VoIP: ISDN Interfaces Configuration 6.3-52
6.3.1 ISDN common parameters 6.3-52

6.3.2 BRI Interface....6.3-55
6.3.3 PRI Interface....6.3-57
6.4 VoIP: E1 R2 interface Configuration....6.4-59
6.4.1 CAS R2 profiles configuration....6.4-59
6.4.2 E1 R2 interface configuration....6.4-62
6.5 VoIP: Internal Local Voice Port Configuration....6.5-64
6.6 VoIP: H.323 Gateway Configuration....6.6-66
6.7 VoIP: SIP Gateway Configuration....6.7-71
6.7.1 Parameters for Signaling....6.7-71
6.7.2 Parameters for Registration....6.7-71
6.7.3 Tuning of SIP Messages....6.7-73
6.7.4 SIP Timers....6.7-75
6.7.5 RTP Parameters....6.7-76
6.7.6 Intrusive voice port mode....6.7-76
6.7.7 Number portability....6.7-78
6.8 VoIP Coder Profiles Configuration....6.8-79
6.9 Voice over IP Dial Peer Configuration....6.9-80
6.9.1 Common Parameters....6.9-80
6.9.2 SIP-Specific Parameters....6.9-85
6.9.3 H.323-Specific Parameters....6.9-89

7 VOICE OVER IP ROUTING TABLE....6.9-92

7.1 VoIP Routing Overview....7.1-92
7.1.1 Introduction....7.1-92
7.1.2 Numbering plan management and routing process....7.1-92
7.1.3 Dial plan management....7.1-92
7.1.4 Wildcards....7.1-93
7.1.5 Regular expressions....7.1-94
7.1.6 Routing process summary....7.1-95
7.1.6.1 Case of a call coming from a local port....7.1-95
7.1.6.2 Case of a call coming from the H.323/SIP Network....7.1-95
7.1.6.3 Total & Partial match....7.1-96
7.1.6.4 Routing Empty Number....7.1-96
7.2 VoIP RoutIng Configuration....7.2-97
7.2.1 Numbering plan description and default type of number....7.2-97
7.2.2 Pre processing management....7.2-97
7.2.3 Dial plan management....7.2-97
7.2.4 Routing table management....7.2-97
7.2.5 Route Configuration....7.2-98
7.2.6 Call distribution....7.2-103
7.2.7 Post processing management....7.2-103
7.3 Use of the routing table for SIP naming....7.3-105
7.3.1 Registration....7.3-105
7.3.2 Call Signaling....7.3-105
7.4 Call Backup Routing Parameters....7.4-106
7.4.1 Backup Criteria: Q.850 Release Causes....7.4-106
7.4.2 Backup Timers....7.4-106

8 VOIP EXAMPLES, STATISTICS AND DEBUG....7.4-107

8.1 VoIP Configuration Examples....8.1-107
8.1.1 Configuration Example....8.1-107
8.1.2 Authentication example....8.1-109
8.1.3 Backup example....8.1-109
8.2 VoIP Statistics....8.2-111
8.2.1 Running Configuration....8.2-111
8.2.2 Voice Hardware and Software versions....8.2-113
8.2.3 Voice global information and memory....8.2-113
8.2.4 ISDN active calls....8.2-113
8.2.5 BRI/S0 Voice Port Statistics....8.2-113
8.2.6 PRI Voice Port Statistics....8.2-114
8.2.7 FXS Voice Port Statistics....8.2-115
8.2.8 FXO Voice Port Statistics....8.2-116
8.2.9 Dial Peer VoIP Statistics....8.2-116
8.2.10 MOS Scoring Statistics....8.2-118

8.2.11 H.323 Gateway Statistics....8.2-118
8.2.12 SIP Gateway Statistics....8.2-119
8.2.13 Events....8.2-119
8.3 VoIP Troubleshooting tools....8.3-122
8.3.1 LEDs....8.3-122
8.3.1.1 ONE200/400 (two "Voice" LEDs)....8.3-122
8.3.1.2 Other ONEXX0 devices (only one "Voice" LED)....8.3-122
8.3.2 ISDN Signaling Capture....8.3-122
8.3.3 Call Generator/Responder....8.3-124
8.3.3.1 Responder....8.3-125
8.3.3.1.1 Configuration....8.3-125
8.3.3.1.2 Details about Responder Signaling....8.3-125
8.3.3.1.3 Details about the RTP Flow....8.3-125
8.3.3.2 Call Generator....8.3-126
8.3.3.2.1 Details about Generator Signaling....8.3-127
8.3.3.2.2 Details about Generator Call Type (Service)....8.3-127
8.3.3.2.3 Example....8.3-128
8.3.3.3 Statistics....8.3-129
8.3.3.3.1 Events....8.3-129
8.3.3.3.2 Displaying Statistics....8.3-129
8.3.4 RTP Call Detailed Reports....8.3-130
8.3.5 VoIP Call Detailed Reports....8.3-132
8.3.6 Protocol Traces....8.3-133

9 SIP PROXY....8.3-134

9.1 Introduction to SIP Proxy....9.1-134
9.1.1 Registrar and Registration to Softswitch....9.1-134
9.1.2 Call Routing....9.1-134
9.1.3 SIP Signaling Translation....9.1-134
9.1.4 NAT ALG....9.1-135
9.1.5 Basic Call Flow....9.1-135
9.2 SIP Proxy Configuration Commands....9.2-136
9.2.1 SIP Server....9.2-136
9.2.2 VoIP dial-peers....9.2-137
9.2.3 Voice-Routing....9.2-137
9.2.4 SIP Proxy with Transcoding Capability....9.2-139
9.2.5 Statistics and Debug....9.2-140
9.2.6 Configuration Example....9.2-140

10 CALL ADMISSION CONTROL (CAC)....9.2-142

10.1 Introduction to CAC....10.1-142
10.1.1 Call Admission....10.1-143
10.1.2 Media Renegotiation....10.1-143
10.2 CAC Configuration and Control....10.2-144

11 MEDIA GATEWAY CONTROL PROTOCOL (MGCP)....10.2-146

11.1 Introduction to MGCP....11.1-146
11.1.1 MGCP Protocol Overview....11.1-146
11.1.1.1 Signaling Processing....11.1-146
11.1.1.2 Call Agent....11.1-146
11.1.1.3 Tones & ringing....11.1-146
11.1.1.4 Caller Identification....11.1-146
11.1.2 Backup....11.1-147
11.1.3 Voice Processing....11.1-147
11.1.3.1 Group 3 FAX Processing....11.1-148
11.1.3.2 Modem Processing....11.1-148
11.1.3.3 DTMF Processing....11.1-148
11.2 MGCP Configuration....11.2-149
11.2.1 Introduction....11.2-149
11.2.2 Configuration....11.2-150
11.2.3 Physical Voice Ports....11.2-150
11.2.3.1 Parameters for Echo Cancellation....11.2-150
11.2.3.2 Parameters for Gain control....11.2-150
11.2.3.3 Parameters for Ringing....11.2-150
11.2.3.4 Parameters for Tones....11.2-151
11.2.3.5 Parameters for Dialing....11.2-151

11.2.4 Internal Local Voice Port (POTS) 11.2-151
11.2.5 MGCP Gateway....11.2-152
11.2.5.1 Parameters....11.2-152
11.2.6 VoIP Coder Profiles....11.2-152
11.2.7 Voice over IP Dial Peer....11.2-153
11.2.7.1 Parameters....11.2-153
11.3 MGCP Configuration Example....11.3-155
11.4 MGCP Statistics Display....11.4-157
11.4.1 FXS Voice Port Statistics....11.4-157
11.4.2 Dial Peer VoIP Statistics....11.4-157
11.4.3 MOS Scoring Statistics....11.4-159
11.4.4 MGCP Gateway Statistics....11.4-159
11.4.5 Events....11.4-160
11.5 MGCP Troubleshooting tools....11.5-161
11.5.1 LEDs....11.5-161
11.5.1.1 ONE200/400 (two "Voice" LEDs)....11.5-161
11.5.1.2 Other ONEXX0 devices (only one "Voice" LED)....11.5-161
11.5.2 MGCP protocol capture....11.5-161
11.5.3 RTP Call Detailed Reports....11.5-161

12 RTP CLOCK SYNCHRONIZATION....11.5-164

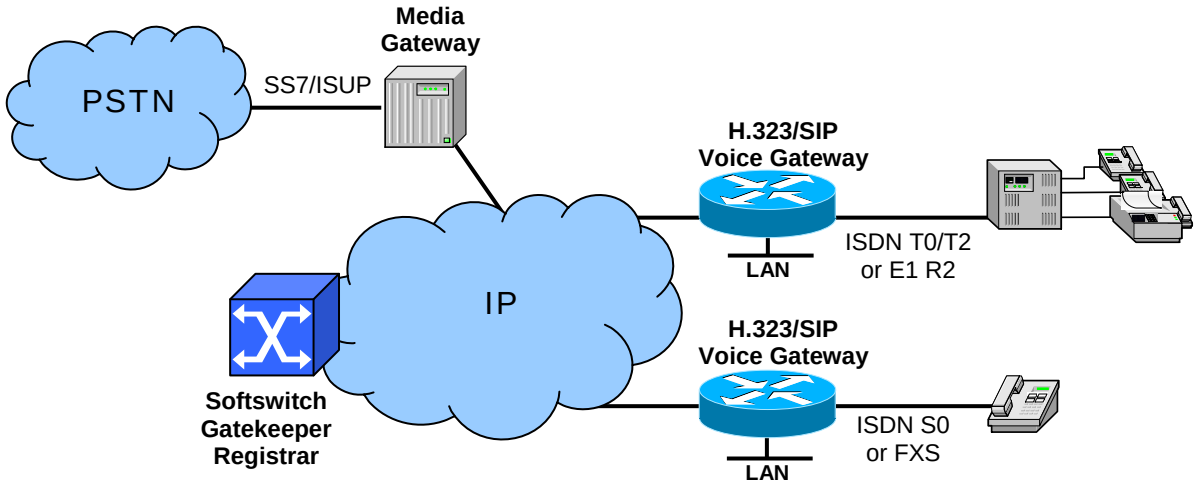
12.1 RTP Clock Synch Overview....12.1-164
12.2 RTP Clock Synch Description....12.2-164
12.3 RTP Clock Synch Algorithm....12.3-165
12.4 RTP Clock Synch Configuration....12.4-168
12.4.1 Voice ports....12.4-168
12.4.2 Peer-to-Peer Mode....12.4-168
12.4.3 Multicast mode....12.4-168
12.5 RTP Clock Synch Statistics....12.5-169

2 VOICE OVER IP

2.1 INTRODUCTION TO SIP & H.323

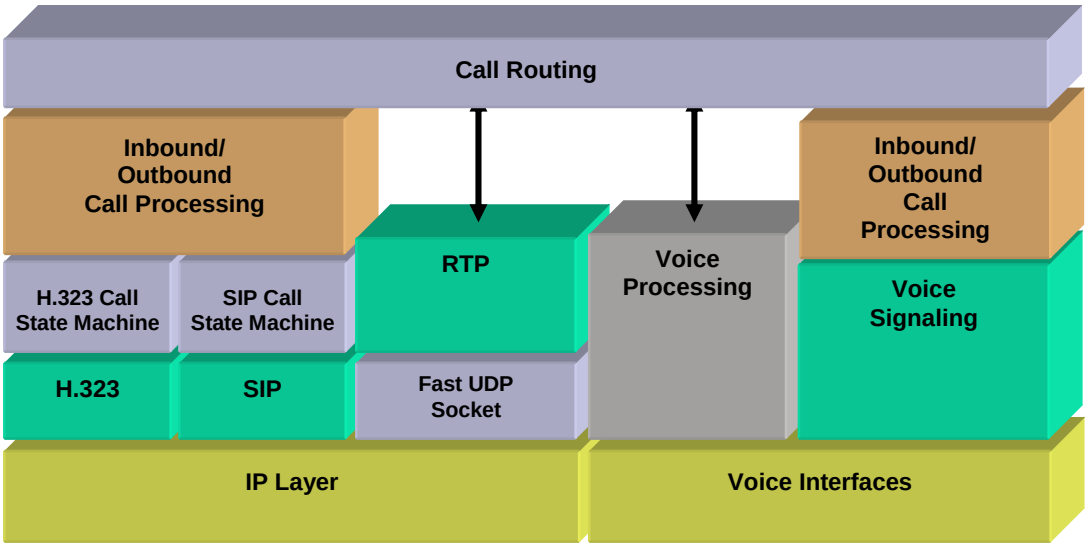
The OneOS-based voice-capable router (i.e. ONEXX0) enables the connection of conventional telephone terminals (ISDN or analog), or PBXs (ISDN BRI/PRI, E1 R2 or analog), to the PSTN through an IP network compliant with ITU-T H.323 v4 and SIP v2. The OneOS-based voice-capable router is a voice gateway and inter-works with all the other devices in the H.323/SIP architecture: IP Phone, Soft Phone on PC (e.g. NetMeeting), Media Gateway, Gatekeeper & Softswitch, Multipoint Control Unit (MCU), Interactive Voice Response server (IVR)...

A typical architecture for a Voice over IP network is as follows:



2.2 SIP AND H.323 OVERALL ARCHITECTURE

The diagram below represents an overview of the VoIP software functional blocks. The diagram shows that the H.323 and SIP gateway function share a common set of functions.



Details about every block:

- Voice interfaces: they are the ports where legacy telephone devices are connected, such as PBX and phones. They are:
  - FXS ports
  - FXO ports
  - E1 R2 ports
  - BRI ports: S0/T0 in NT/TE mode
  - PRI ports: S2/T2 in NT/TE mode
- Voice signaling: it is the processing of the ISDN signaling/analog signaling so that calls are translated into an internal call format. An ISDN decoder enables ISDN signaling decoding.
- Inbound/outbound call processing: phone number translation before/after routing, dialed number pattern matching to start calling in case of received overlap dialing.
- Voice processing: the DSP software makes the voice call compression, mode/fax detection, fax modulation/demodulation, DTMF tone detection/generation, silence detection, echo cancellation, tone generation, in-band FXS caller-id generation.
- The RTP processing is directly managed in DSP, which includes RTP frame formatting and buffering (dynamic jitter buffer). Having such processing embedded in the DSP software allows a more accurate real-time processing.
- Fast UDP socket: tuned UDP socket for higher performance routing.
- SIP/H.323 call state machines: this layer manages internal call state in OneOS and maps call information elements into SIP/H.323 specific formats and vice-versa.
- SIP/H.323 stack: handle VoIP signaling for the required standard.
- Call routing: call routing determines the output path of a received call. The output path is either a VoIP remote peer or a voice interface port. Local call switching is possible (call switching between two voice interface ports or between two VoIP peers). Backup routing permits the following: if a call fails on the primary route, a call attempt is placed on the backup route. Call routing can select the VoIP coding profile and manage number portability (availability of this feature is submitted to certain restriction). Call routing between the following devices is not supported: H.323 => H.323, SIP => SIP, SIP => H.323, and H.323 => SIP.

3 H.323 PACKET-BASED MULTIMEDIA COMMUNICATIONS SYSTEMS

3.1 H.323 PROTOCOL OVERVIEW

3.1.1 H.323 Signaling Processing

The OneOS-based voice-capable router implements the H.323 protocol in conformance with:

- ITU-T H.323 v4 "Packet-based multimedia communications systems"
- ITU-T H.225.0 "Call signaling protocols and media stream packetization for packet-based multimedia communication systems"
- ITU-T H.235 "H.323 security framework"
- ITU-T H.245 "Control protocol for multimedia communication"
- ITU-T H.323 Annex D for FAX "Real-time facsimile over H.323 systems"

The OneOS-based voice-capable router supports the following features:

- RAS protocol with Gatekeeper discovery, registration, admission, disengage. The RAS protocol can be disabled; a static routing table translating the called number in the remote H.323 device address is configurable (with optional number transformation).
- H.225/Q.931 protocols for call signaling. En-bloc and overlap sending modes are both supported.
- H.235 for authentication (RAS only).
- H.245 protocol for media channel is supported. The fast-start (or fast-connect) procedure is also supported to reduce the signaling traffic.

3.1.2 Use of a Gatekeeper

The OneOS-based voice-capable router supports the gatekeeper discovery, registration and admission / disengagement. The OneOS gateway can be authenticated by means of the H.235 protocol.

All these parameters are configurable for discovery and registration:

- Gatekeeper identifier: used for discovery and registration. It is generally used to identify a gatekeeper in charge of a local zone.
- Gatekeeper IP address: it must be specified if the automatic discovery using RAS; multicast is not used.
- H.323 identifier (also called "alias"): alphanumeric string identifying the OneOS-based voice-capable router in the gatekeeper. It can be configured globally (see h323-gateway command) and/or for each local port (in the routing table).
- Gateway prefix: prefix (with optionally "#" and "*****" characters) indicating to the gatekeeper that all the calls having the same destination number pattern must be routed to that gateway. It can be configured globally (see h323-gateway command) and/or for each local port (in the routing table).

3.1.2.1 Resource Management (RAI)

It is possible to enable the resource management using the RAI message. This feature is used by a Gatekeeper to manage a pool of gateways: the incoming calls are routed on the gateway, which is not becoming busy. Two criteria are defined and can be combined:

- Number of time-slot, which are currently used (on enabled voice ports only). For example, a RAI "on" can be sent if more than 70% of the B channels of the PRI ports are used.
- Bandwidth used (mainly for the RTP flows, depending on the voice coders). A maximum bandwidth that can be used by the H.323 gateway is configurable. For example, a RAI message can be sent if more than 80% of the authorized bandwidth is used.

3.1.2.2 Intrusive mode

It is possible to enable a logical link between the state (layer 1) of the voice ports and the registration. This feature allows the gatekeeper to know if a gateway is operational before sending a call to it. Two modes are possible: all the voice-port must be up to start registration, one of the ports must be up to start the registration. The voice ports list to be checked is configurable.

This feature also allows the PBX to know if the VoIP service is up or down: the ISDN interface physical layer is set at a down state if the H.323 gateway is not registered. In such case, the PBX can route the calls to other ISDN interfaces for backup.

3.1.3 Application Cases

- For a PBX application with BRI interfaces, a global H.323 identifier or a Gateway prefix should be sufficient due to PBX facilities that can switch different phone calls independent of the BRI Interface.
- For analog ports application connecting subscribers, it could be necessary to indicate to the gatekeeper an E.164 number for each port.

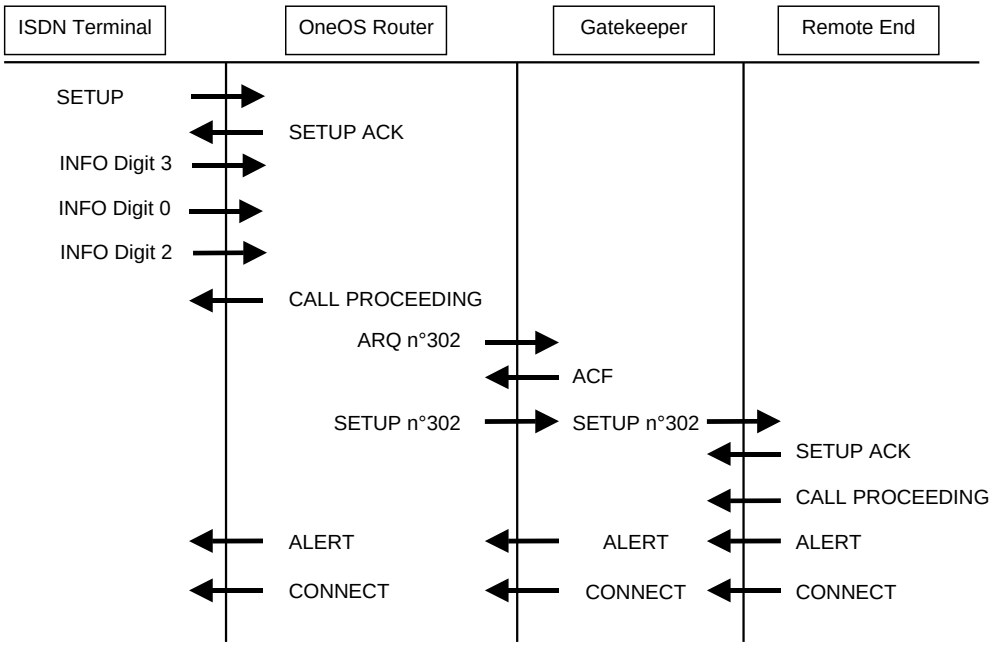
3.2 H.323 – ISDN SIGNALING GATEWAY

3.2.1 Dialing

Two modes are possible: en-bloc dialing and overlap dialing.

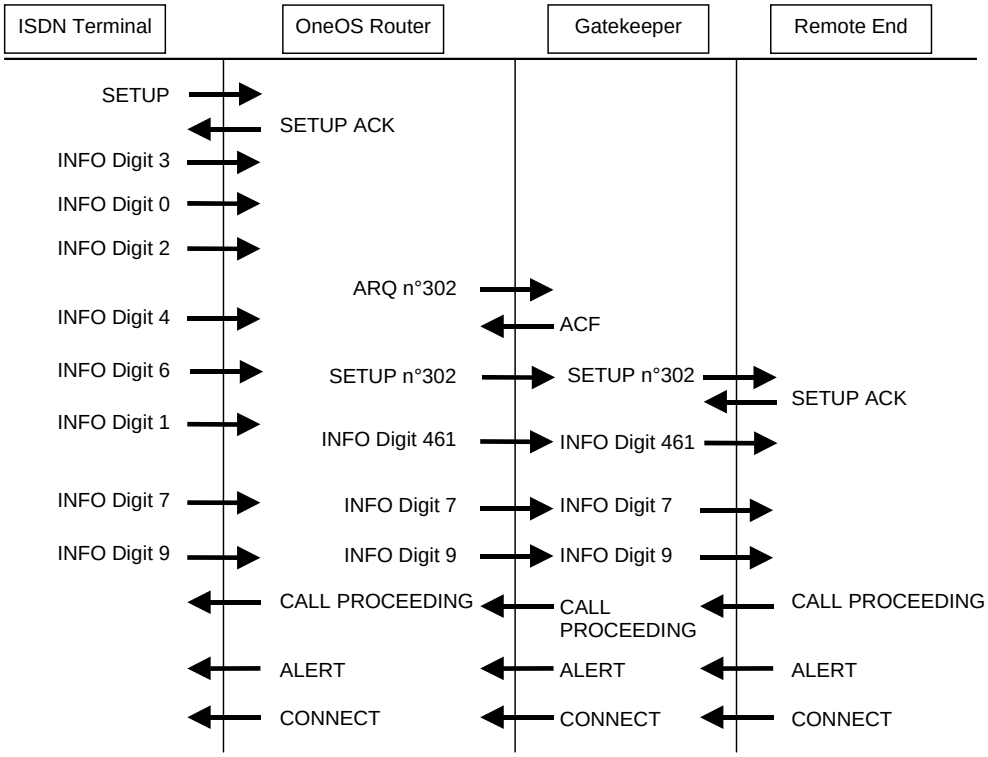
- The en-bloc dialing functions as follows: the complete destination number is inserted in the SETUP message. If a gatekeeper is used, an admission request providing the called number is sent to the gatekeeper that returns the IP address to be contacted for signaling. If a gatekeeper is not used, the called number is compared with the E.164 prefix configured in the routing table. If the called number matches an entry in the routing table, an H.225/Q.931 SETUP message is sent to the remote H.323 device.
- The overlap dialing functions as follows: the called number is sent digit by digit from the terminal. The routing table contains parameters to determine the criteria to be used to consider the number as "routable". The criteria can be the length (i.e. the number of digits must reach a certain length, which can be null for full transparency of the overlap dialing) or a timeout (the device awaits digits for a certain time) and can depend on the beginning of the number (consequently, several number formats can be used). A "routable" number can be considered as "complete" or not: if not, overlap dialing will be possible end-to-end. The "routable" number is used for admission request if a gatekeeper is used.

Example of ISDN overlap dialing and H.323 en-bloc dialing with a length of 3 digits for routing:



Note: The CALL PROCEEDING is sent by the OneOS-based voice-capable router to avoid a timeout on the terminal side due to an excessive time required by gatekeeper admission and SETUP message emission. The SETUP message is sent by the OneOS-based voice-capable router to the gatekeeper, because routed signaling is used. It is possible the SETUP is sent to the remote device in non-routed mode.

Example of end-to-end overlap dialing with a length of 3 digits for routing:



Note: The OneOS-based voice-capable router supports also overlap dialing for incoming calls (from H.323 to ISDN terminal). The signaling is routed through the gatekeeper.

3.2.2 Ringback tones and announcements

The OneOS-based voice-capable router generates a configurable dialing tone (on the B channel) in case of overlap dialing until the reception of the first digit.

When the SETUP message is sent to the H.323 remote end, the remote end can behave in three different ways:

- The remote endpoint sends a CALL PROCEEDING or ALERT message with the Information Element (IE) "Progress" with "in-band" as information. Additionally, the RTP channel is established without waiting for full call establishment and the ISDN B channel is open. This method allows the remote H.323 device to send specific tones (such as customized ringback tones) or vocal announcements.
- The remote endpoint sends a CALL PROCEEDING or ALERT message with the Information Element (IE) "Progress" with "in-band" as information. But the RTP channel is not open, though. The ISDN B channel is open even though the RTP channel is not open. The ringback tone is generated locally.
- The remote end does not send an Information Element with "Progress In-band": the OneOS-based voice-capable router sends a ringback tone in the B channel when receiving the ALERT message from the remote end. The RTP channels will be opened after the connection (the remote endpoint off-hooks the phone).

3.2.3 Disconnection

The OneOS-based voice-capable router can also receive a "Progress In-band" IE in the RELEASE COMPLETE message: it allows the remote H.323 device to indicate that there is a vocal announcement. The RTP channels are not disconnected and the OneOS-based voice-capable router waits for a disconnection from the ISDN terminal (a timer set at 30 seconds is used by the OneOS-based voice-capable router in case of non disconnection).

The OneOS-based voice-capable router can optionally generate itself release tones in the B channel. It inserts then a "Progress In-band" information element. This feature is used if the PBX is not able to generate an appropriate tone to the user.

3.2.4 Advice of charge

The OneOS-based voice-capable router is able to send charging information on ISDN port. The provisioning can be done for each voice-port (for AOC-D and AOC-E) if the terminal is not able to request the service by itself. The charging information comes from the remote H.323 softswitch with two possible formats: ETSI or ECMA. The OneOS-based voice-capable router translates the information into the ETSI or EuroNumeris format towards the ISDN terminal.

The AOC-E (end of call) charging information can be computed by the OneOS-based voice-capable router itself if the softswitch does not support it.

3.2.5 Complementary Services

The complementary services are relayed transparently between ISDN and H.323.

Note: whatever the configuration and/or the "octet 3a" value received, the calling number is not suppressed or modified by the OneOS-based voice-capable router (except with the number translation facility).

3.3 H.323 ANALOG PORT SIGNALING

3.3.1 Dialing

When detecting an off-hook, the OneOS-based voice-capable router emits a configurable dialing tone until the reception of the first digit. If no digit is received within a configurable delay, a busy tone is sent and the OneOS-based voice-capable router waits for an on-hook.

As an alternative, the OneOS-based voice-capable router can send a call with a pre-configured number when detecting an off-hook condition (direct call).

The destination number is sent digit by digit by the terminal. The routing table contains parameters to determine the criteria making the number "routable". The criteria can be the length (i.e. the number of digits must reach a certain length which can be null for full transparency of the overlap dialing) or a timeout (the device awaits digits for a certain time) and can depend on the beginning of the number (consequently, several number formats can be used). A "routable" number can be considered as "complete" or not (configurable in the routing table): if not, overlap dialing will be possible end-to-end. The "routable" number is used for admission request if a gatekeeper is used.

3.3.2 Tones & Announcements

The OneOS-based voice-capable router behavior is similar to the one described for ISDN terminals.

3.3.3 Ringing

In case of incoming call, a Ringing signal is sent to the terminal. The ringing signal is fully configurable. A configurable timer limits the ringing duration without detection of an off-hook.

3.3.4 Caller Identification

The OneOS-based voice-capable router generates the appropriate information about the caller number during the ringing signal. Two modes are supported: FSK or DTMF. The initial ringing duration is configurable.

3.3.5 H.245 Terminal Capabilities

The OneOS-based voice-capable router sends a configurable list of coders in the terminal capability message (or in the SETUP message in Fast Connect mode). For each coder, the timestamp must be indicated.

3.3.6 Advice of charge

The OneOS-based voice-capable router is able to send charging information on analog port by using several methods: 12/16 KHz pulse, polarity inversion or ETSI-compliant advice of charge. The provisioning can be done for each voice-port.

3.3.7 Line Power Drop

The FXS line power is forced off when the port is in "shutdown" state. It is possible to shut down the port if the VoIP gateway is not operational (available for SIP only). This feature is mainly used for alarm devices. See the `intrusive-voiceport` command in `sip-gateway` parameter group, for more details. Some timers are configurable for each port: see the `fxs-power-timeout` in `voice-port` parameter group for more details.

3.4 H.323 FXO PORT SIGNALING

3.4.1 Outgoing Call

When voice routing is configured such that a call must be routed to a FXO port, the OneOS-based voice-capable router first makes an off-hook transition that indicates to the network that the subscriber is going to dial. Then, the first digits are sent after a configurable time. There is no detection of dial tone before sending the digits: there will not be any call failure due to a wrong tone configuration.

The number is sent digit-by-digit. The digit duration and the time between two consecutive digits are configurable.

After sending the last digit, the voice path is established and the call is considered as connected. There is neither ring back tone detection nor polarity reversal detection.

3.4.2 Incoming Call

The ringing signal of an incoming call is detected after the configurable number of ringing pulses. The Caller Identification is not supported; in other words, the calling number is unknown.

Upon ringing signal detection, two behaviors are possible, depending on the configuration:

1. First behavior called "second-step dialing": in this mode, the FXO port goes directly to the off-hook state and works as a FXS port for the dialing reception (a dial-tone is transmitted). The received digits are processed through the routing table until a match is found. If a match is found, the call is routed to the appropriate subscriber.
2. Second behavior called "direct routing": the call is routed to a predefined port. The off-hook state is set when the call is connected. In case of remote disconnection, successive off-hook / on-hook signals notify the disconnection to the calling party (fixed duration: 1 second).

If direct routing is not configured and no route is found in second step dialing mode, the incoming call is disconnected by successive off-hook / on-hook signals (fixed duration: 1 second).

4 SIP SESSION INITIATION PROTOCOL

4.1 SIP PROTOCOL OVERVIEW

4.1.1 SIP Signaling Processing

The OneOS-based voice-capable router implements the SIP protocol in conformance with:

- RFC 2327: Session Description Protocol (SDP). Describes how to negotiate and establish the media channels.
- RFC 3204: MIME media types for ISUP and QSIG Objects. Describes how to transport SS7 / QSIG layer 3 messages to a call agent.
- RFC 3261: Session Initiation protocol (SIP). Describes how to open and to close a session between two peers with or without a proxy / call Agent.
- RFC 3323: A Privacy Mechanism for the Session Initiation Protocol (SIP).
- RFC 3325: Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks.
- RFC 3372: SIP for Telephones (SIP-T): Context and Architectures. Specifies the use of SIP for an old telephony network. Gives example for an ISUP/SS7 to SIP translator. This RFC can be used for information about how to make interworking between ISDN and SIP.
- RFC 3459: Critical Content Multi-purpose Internet Mail Extensions (MIME) Parameter. Update of the RFC 3204, providing complementary information.
- RFC 3515: The Session Initiation Protocol (SIP) Refer Method.
- RFC 3665: Session Initiation Protocol (SIP) Basic Call Flow Examples. Gives examples for a minimum SIP implementation.
- RFC 3666: Session Initiation Protocol (SIP) Public Switched Telephone Network (PSTN) Call Flows. Gives examples of call flows for ISUP and ISDN interworking.

The following SIP messages are supported: INVITE (RE-INVITE), ACK, REGISTER, CANCEL, OPTIONS, UPDATE, PRACK, and NOTIFY.

4.1.2 Dialog with SIP-Proxy

The OneOS-based voice-capable router supports the registration to a SIP registrar and can function with several SIP proxies. You can define an alternate registrar for backup and Keepalive values to check access to the SIP proxy and registrar.

4.1.3 Dialog via Outbound Proxy

The OneOS-based voice-capable router can optionally send all the Registration and/or call signaling messages to an outbound proxy. Generally, this feature is required when a Session Border Controller is used. The packet payload containing SIP signaling is addressed to the proxy but the IP packet destination address is the IP address of the outbound proxy.

4.1.4 Voice Path Establishment

The RTP flows are established in two-way mode when the 200OK message is sent and ACK received.

Sometimes, tones and announcements may be sent before the call connection. It may be necessary to get all the SDP information before the 200OK/ACK exchange.

The use of SDP in 1xx message is allowed by a specific configuration parameter and has the following effects:

- SIP→ISDN call: a SDP part will be added if a Progress In-band IE is received on the ISDN port.
- For ISDN→SIP call: the SDP part of a 1xx message will be processed and translated to an IE progress in-band towards the ISDN port.
- For SIP outgoing calls: whatever the SDP in 1xx message is used or not, the OneOS-based voice-capable router is able to receive any RTP flow just after sending the INVITE message (it includes a SDP part). The RTP flow will be sent by the OneOS-based voice-capable router as soon as a SDP part is received.
- For SIP incoming calls: the OneOS-based voice-capable router can send the SDP information in 180/183 message (if configured and presence of IE progress In-band) or will send it in the 200OK. It is ready to receive RTP flow at this stage. It will send RTP flow as soon as it has sent and receive SDP information.

PRACK message is also supported: it may be required by to SIP proxy to send RTP flow before the connection.

4.1.5 "From", "To" and "Contact" fields configuration

For the "From", "To" and "Contact" fields, the following parameters are configurable:

1. sip-username: SIP identifier
2. hostname: domain name or IP address
3. authentication: username & password

A local subscriber is identified by sip-username@hostname. The sip-username is generally the phone number but it can be replaced by a name (routing table configuration). The hostname can be written as an IP address or a configurable name (global choice in the SIP gateway configuration or configured in the routing table).

The routing table is scanned during registration: dial-peer pots including the "ua-sip" option are registered with the prefix or a configurable sip-username and hostname. Specific usernames and passwords can be defined for authentication. The SIP gateway can also register with a global configurable sip-username and hostname.

The calling number is searched in the routing table when a call is received on a local port. If found (match with dial-peer pots and prefix), an optional sip-username and hostname may replace the number and a specific username & password can be used for authentication. For a call coming from a SIP proxy, the username in the "To" field can also be translated to a phone number.

The "To" field is built with the destination phone number and a domain name or IP address. The phone number can optionally be replaced by a name (sip-username) if configured in the routing table. The domain name or IP address is the SIP proxy address.

4.1.6 Mapping of Release Causes

If the SIP response releasing the call contains a reason header (RFC 3326), the Q.850 release cause of that header is used as ISDN release cause.

When an ISDN → SIP call is released by the SIP network before the call is established, the SIP response code (4xx, 5xx, 6xx) is mapped into an ISDN release cause as specified by the table below:

SIP Response Code	ISDN Cause	
	N°	Definition
400 Bad Request	127	Not specified
401 Unauthorized	127	Not specified
402 Payment Required	127	Not specified

SIP Response Code	ISDN Cause	
	N°	Definition
403 Forbidden	127	Not specified
404 Not Found	1	Unallocated (unassigned) number
405 Method Not Allowed	127	Not specified
406 Not Acceptable	127	Not specified
407 Proxy Authentication Required	127	Not specified
408 Request Timeout	127	Not specified
410 Gone	22	Number changed
413 Request Entity Too Large	127	Not specified
414 Request-URI Too Long	127	Not specified
415 Unsupported Media Type	127	Not specified
416 Unsupported URI Scheme	127	Not specified
420 Bad Extension	127	Not specified
421 Extension Required	127	Not specified
423 Interval Too Brief	127	Not specified
480 Temporarily Unavailable	20	Subscriber absent
481 Call/Transaction Does Not Exist	127	Not specified
482 Loop Detected	127	Not specified
483 Too Many Hops	127	Not specified
484 Address Incomplete	28	Invalid number format (address incomplete), except with a route including the 'overlap' option
485 Ambiguous	127	Not specified
486 Busy Here	17	User busy
487 Request Terminated	16	Normal Call clearing
488 Not Acceptable Here	127	Not specified
491 Request Pending	127	Not specified
493 Undecipherable	127	Not specified
500 Server Internal Error	127	Not specified
501 Not Implemented	127	Not specified
502 Bad Gateway	27	Destination out of order
503 Service Unavailable	127	Not specified
504 Server Time-out	127	Not specified
505 Version Not Supported	127	Not specified
513 Message Too Large	127	Not specified
580 Precondition Failure	127	Not specified
600 Busy Everywhere	17	User busy
603 Decline	21	Call rejected
604 Does Not Exist Anywhere	1	Unallocated (unassigned) number
606 Not Acceptable	127	Not specified

Note: the default mapping can be modified using the `sip-to-isdn-cause` command.

When a SIP → ISDN call is released before call establishment, the ISDN release cause is mapped into the following SIP responses:

Outgoing calls		
ISDN cause		SIP Response Code
N°	Definition	
1	Unallocated (unassigned) number	404
2	No route to specified transit network	500
3	No route to destination	500
6	Channel unacceptable	500

Outgoing calls		
ISDN cause		SIP Response Code
N°	Definition	
7	Call awarded and being delivered in an established channel	500
8	Preemption	500
16	Normal Call clearing	487
17	User busy	486
18	No user responding	480
19	No answer from user (user alerted)	480
20	Subscriber absent	480
21	Call rejected	480
22	Number changed	410
26	Non-selected user clearing	480
27	Destination out of order	502
28	Invalid number format (address incomplete)	484
29	Facility rejected	500
30	Response to STATUS ENQUIRY	500
31	Normal, unspecified	480
34	No circuit/channel available	480
38	Network out of order	500
39	Permanent frame mode connection out of service	500
40	Permanent frame mode connection operational	500
41	Temporary failure	500
42	Switching equipment congestion	500
43	Access information discarded	500
44	Requested circuit/channel not available	500
46	Precedence call blocked	500
47	Resource unavailable, unspecified	500
49	Quality of service not available	500
50	Requested facility not subscribed	500
57	Bearer capability not authorized	500
58	Bearer capability not presently available	500
62	Inconsistency in designated outgoing access information and subscriber class	500
63	Service or option not available, unspecified	500
65	Bearer capability not implemented	500
66	Channel type not implemented	500
69	Requested facility not implemented	500
70	Only restricted digital information bearer capability is available	500
79	Service or option not implemented, unspecified	500
81	Invalid call reference value	500
82	Identified channel does not exist	500
83	A suspended call exists, but this call identity does not	500
84	Call identity in use	500
85	No call suspended	500
86	Call having the requested call identity has been cleared	500
87	User not member of CUG	500
88	Incompatible destination	500
91	Invalid transit network selection	404
95	Invalid message, unspecified	500
96	Mandatory information element is missing	500
97	Message type non-existent or not implemented	500

Outgoing calls		
ISDN cause		SIP Response Code
N°	Definition	
98	Message not compatible with call state or message type non-existent or not implemented	500
99	Information element /parameter non-existent or not implemented	500
100	Invalid information element contents	500
101	Message not compatible with call state	500
102	Recovery on timer expiry	480
110	Message with unrecognized Parameter, discarded	500
111	protocol error, unspecified	500
127	interworking unspecified	480

4.2 SIP COMPLEMENTARY SERVICES

In bridge mode, with regard to complementary services, all headers (refer to next chapters for each service) are relayed except:

- Caller identity can be modified by routing process and pre/post processing.
- CLIR is applied from SIP proxy to SIP server.
- Headers may be overwritten if trunking mode is in force.

In back to back mode, the behavior is similar to SIP to ISDN call followed by ISDN to SIP call (refer to next chapters).

In the following "P-Asserted-Identity" and "P-Preferred-Identity" header fields are mentioned.

"P-Asserted-Identity" header field is used to provide the user identity authenticated by a trusted SIP entity (network provided) and "P-Preferred-Identity" header field is the preferred user identity (the one to be asserted) used to authenticate against the trusted SIP entity (user provided).

The standard behavior for SIP phones is to put the user identity into the "From" header field.

The standard behavior for SIP public network is to put the identity provided by the user into the "From" header field and optionally into the "P-Preferred-Identity" header field and to put the asserted identity (authenticated) provided by the network into the "P-Asserted-Identity" header field.

4.2.1 SIP/FXS interworking

With SIP, advanced complementary services are provided on FXS devices: Call waiting, CLIP / CLIR, Hold / Retrieve, Brokering, Attended Call Transfer, Explicit Call Transfer, Message Waiting Indication, 3-party conferencing.

Refer to 6.2.4.2 for more details about SIP/FXS complementary services interworking.

4.2.2 SIP/ISDN interworking

With SIP, advanced complementary services are also provided on ISDN devices (Euro-ISDN only): Call forwarding (CFU, CFNR, CFB), CLIP/CLIR, COLP/COLR, Hold / Retrieve, Suspend / Resume, Attended Call Transfer, Explicit Call Transfer, Call deflection, Call rerouting, Message Waiting Indication, 3-party conferencing, User-to-user signaling (UUS).

The following chapters describe the SIP/ISDN complementary services interworking. Note that the general cases are described knowing that pre-processing, routing process and post-processing as well as trunking mode have impact on several parameters (calling and called numbers format, type of number, numbering plan, etc.).

4.2.3 CLIP/CLIR Complementary Services

4.2.3.1 CLIP Complementary Service

The ISDN CLIP service (Calling Line Identification Presentation, also known as Calling Number Identification – CNID) is a called party feature that transmits the calling number (the caller identity) to the called party when the call is being set up.

With SIP, CLIP is provided by the URI in the "From" header field.

4.2.3.2 CLIR Complementary Service

The ISDN CLIR (Calling Line Identification Restriction) is a calling party feature that prevents presentation of the calling number to the called party. The presentation code and the screening indicator are provided in octet 3a of the Q.931 calling number information element. The presentation code can take the following values: presentation restricted (1) or number not available (2). The screening indicator can take the following values: user provided, not screened (0) or user provided, verified and passed (1) or user provided, verified and failed (2) or network provided (3).

With SIP in same cases, CLIR can be user provided. The calling party hides the CLIP information directly in the "From" header field and eventually in the "P-Preferred-Identity" header field. Example:

```
From: <sip:anonymous@anonymous.invalid>
```

With SIP in most cases, CLIR is provided by the network. "Privacy" header field (with parameter "user") is used by a privacy service on request of the user to hide the CLIP information found in "From" header field. Example:

```
From: <sip:+33123456789@example.com>
Privacy: user
```

"Privacy" header field (with parameter "id") is also used by a privacy service on request of the user to hide the CLIP information found in "P-Asserted-Identity" header (RFC 3325). Example:

```
P-Asserted-Identity: <sip:+33123456789@example.com>
Privacy: id
```

CLIR is handled directly in the "Diversion" header field.

Additionally, the routing table makes it possible to overwrite the Calling Line Identification Restriction. For example, it is possible to enable the CLIR for calls coming from a specific local port or specific calling number.

4.2.3.3 CLIP/CLIR interworking process in SIP to ISDN call

Calling number found in SIP "From" header field is mapped to ISDN "Calling Party Number" Information Element (IE 6C) with Screening Indicator field (octet 3a) set to "User-provided, not screened".

Calling number found in SIP "P-Asserted-Identity" and/or "P-Preferred-Identity" header fields is mapped to another ISDN "Calling Party Number" Information Element (IE 6C) with Screening Indicator field (octet 3a) set to "Network-provided".

SIP "Privacy" header field is mapped to ISDN Presentation Indicator field (octet 3a) set to "Presentation restricted". If `clip-privacy-uri incoming` is in force, the anonymous URI found is also mapped to ISDN Presentation Indicator field (octet 3a) set to "Presentation restricted".

SIP "Diversion" header fields are mapped to ISDN "Redirecting Numbers" Information Elements (IE 74).

4.2.3.4 CLIP/CLIR interworking process in ISDN to SIP call

Calling number found in first ISDN "Calling Party Number" Information Element (IE 6C) is mapped to "From" header field.

ISDN Presentation Indicator field (octet 3a) set to "Presentation restricted" is mapped to SIP "Privacy" header field with id and user parameters. If `clip-privacy-uri outgoing` is in force, the anonymous URI overrides the URI in SIP "From" header field.

Calling numbers found in ISDN "Redirecting Numbers" Information Elements (IE 74) are mapped to SIP "Diversion" header fields (several instances).

4.2.4 COLP/COLR Complementary Services

4.2.4.1 COLP Complementary Service

The ISDN COLP service (Connected Line Identification Presentation) is a calling party feature that transmits and presents the called party identity to the caller when the call is being answered.

With SIP, COLP is provided by the URI in the "P-Asserted-Identity" and/or "P-Preferred-Identity" header fields of the SIP Response.

4.2.4.2 COLR Complementary Service

The ISDN COLR service (Connected Line Identification Restriction) is a called party feature that prevents presentation of the called party identity to the calling party.

With SIP, COLR is provided by the network. "Privacy" header field (with parameter "id") is used by a privacy service on request of the user to hide the COLP information found in "P-Asserted-Identity" header field and in "P-Preferred-Identity" header field.

4.2.4.3 COLP/COLR interworking process in SIP to ISDN call

Called number found in SIP "P-Asserted-Identity" header field is mapped to ISDN Connected Number Information Element (IE 4C) with Screening Indicator field (octet 3a) set to "Network-provided".

Called number found in SIP "P-Preferred-Identity" header field is mapped to ISDN Connected Number Information Element (IE 4C) with Screening Indicator field (octet 3a) set to "User-provided, not screened".

SIP "Privacy" header field is mapped to ISDN Presentation Indicator field (octet 3a) set to "Presentation restricted".

4.2.4.4 COLP/COLR interworking process in ISDN to SIP call

Connected number found in first ISDN "Connected Number" Information Element (IE 4C) is mapped to "P-Preferred-Identity" header field.

ISDN Presentation Indicator field (octet 3a) set to "Presentation restricted" is mapped to SIP "Privacy" header field with id and user parameters.

4.2.5 UUS Complementary Service

4.2.5.1 UUS ISDN service

The ISDN UUS service (User-to-User Signaling, specified in EN 300 286-1) is a feature that allows a party to send/receive a limited amount of information to/from another party over the signaling channel in association with a call to the other party.

UUS1, UUS2 and UUS3 services are supported. The explicit mode (mandatory for UUS2 & UUS3 and optional for UUS1) requires a negotiation between the two ISDN entities.

4.2.5.2 UUS interworking process

With SIP, User-to-User Information (UUI) element can be transported with two methods (regarding the ability of the SIP network to forward or not the information):

- Using the user-to-user header (RFC draft-johnston-sipping-cc-uui – IMS/TISPAN ETSI TS 183 036).
- Using a proprietary application/MIME part in raw mode.

Two modes of operation are offered:

- End-to-end negotiation: the FACILITY messages are forwarded transparently in the application part of the SIP messages. The negotiation is directly achieved between the two ISDN devices. SIP INFO messages are used for that purpose when there is no signaling message. It is important to notice that SIP proxies or VoIP networks must be able to forward SIP INFO messages at any stage of the call and must be transparent to proprietary MIME part of SIP message.
- Local negotiation: the negotiation is achieved locally depending on the configuration. This mode must be used if the SIP network does not support proprietary MIME part of SIP message. Note that in this software release, only the end-to-end negotiation mode is supported.

The UUS services supported by an ISDN port are configurable. If the end-to-end mode is selected, the FACILITY messages are just filtered or not depending on the configured UUS services.

The UUS services supported by the SIP network (or peer) are also configurable. The ability of the SIP network to support SIP INFO messages at any stage of the call is configurable as well.

5 VOIP CALL ROUTING AND VOICE PROCESSING

5.1 VOIP CALL ROUTING

The call is routed using one of two possible methods:

- Implicit routing: all the calls are routed to a local port or to a remote H.323/SIP device, without any analysis of the called number.
- Routing table: the destination number is compared with a list of configured number prefixes. The destination port (local port or remote VoIP peer) is found if the called number matches with one of the prefixes. If a gatekeeper is not used, the routing table may directly include the IP address of the called VoIP device (SIP or H.323 gateway/terminal).

The routing table defines also the numbering plan for overlap dialing (number length depending on the prefix) and identifiers for registration to the gatekeeper (for local ports only).

Several cases are to be considered:

- Case of ISDN calls in en-bloc mode routed to a VoIP device using a softswitch. In this case, the implicit routing is sufficient.
- Case of ISDN calls in overlap dialing mode or analog calls with the necessity to record several digits before sending an admission request to a softswitch. In this case, the routing table must be used to precise the number length.
- Case of calls without a softswitch. Except in case of trunking, the routing table is required to determine the destination VoIP device by an IP address.

The order of the configured routing rules is important: the rule number one is tested first, and then the rule number two, etc. For a call coming from a local port, the rules indicating a VoIP device are checked before the rules indicating a local port. For a call coming from a VoIP device, the rules indicating a VoIP device are not checked.

Once a routing rule matches the called number, the outbound port is determined and also the IP address if the port indicates a VoIP device. The called number can be transformed by suppressing and/or adding digits.

5.1.1 Incoming Call Routing

For each incoming call, the routing is broken down into two phases: first to apply some special actions for the incoming call, then the outgoing port is selected. The first routing phase can be used:

- To make specific number translations on the calling & called number.
- To determine the dial-peer VoIP to be used (and therefore the voice coding profile). (For calls coming from H.323/SIP only).
- Optionally, to define a specific number intended for the reboot of the device (locally or remotely) for maintenance purpose.

5.1.2 Call distribution

The routing table specifies a group identifier. Each port belongs to a group: this feature enables the definition of several interfaces with the same number (very common situation with a PBX connected with

several BRI ports). For each port, a priority inside the group can be defined. When ports have the same priority, a circular selection is made (round robin) or the port with least load in selected (load balancing).

Example for round robin: Port 1: priority 1, Port 2: priority 2, Port 3: priority 2, and Port 4: priority 2. The call is routed to port 1 if available. If not available, the call is routed to port 2 then ports 3, 4, 2, 3 ... and so on.

5.1.3 Call Hunting

It is possible to enable a call hunting for a group (see the routing table configuration). If enabled, a call routed to this group, is sent to each interface of the group until a successful call (including normal failure causes, for example, wrong number or user busy). The up interfaces are tried first, and then the down interfaces if no up interface is available. The call is released if all the interfaces of the group have been unsuccessfully tried.

A BRI interface is declared down if a call is unsuccessful (with a Q.850 release cause greater than 31). It is declared up at startup and after a successful call. Call hunting may be used for backup: if a BRI interface is down, the call is sent again (after two seconds) to another interface inside the same group.

The call hunting is disabled in case of overlap dialing.

5.1.4 Backup Call Routing

A backup call routing is possible in case of outgoing call failure. The criterion is simple: the ITU-T Q.850 cause value must be different from a class 0 or 1, which are expected type values in normal cases. A typical application is backup call routing of the VoIP network by a legacy ISDN network: the main route is VoIP and in case of IP network failure (uplink disconnected, unreachable softswitch...), the call is routed to the ISDN network connected to a S0 / S2 interface.

This feature is configured in the routing table.

5.1.5 Number Translation

It is possible to configure translations on the calling and/or called number.

5.1.5.1 Calling Number Translation on Local Ports

Parameters attached to each local port enable suppression of the calling number or insertion of a prefix in the calling number of the call coming from the local device. The same actions will be applied on the "Connected number" of a CONNECT message coming from the local device.

Insertions in calling numbers are used for example to add a prefix identifying a PBX to a local phone number: a local user identified by "3007" will be identified as "0141873007" in the VoIP network in case of outbound call, by inserting the prefix "014187".

5.1.5.2 Calling & Called Number Translation by Using the Routing Table

The routing table offers the possibility to make translations on the calling and/or called number: prefix suppression & insertion, suffix suppression & insertion. It is also possible to configure specific translations of any patterns in the calling and/or called number.

The main benefit is to define translation for specific numbers (calling and called) only.

The translation can be defined for the incoming routing and/or outgoing routing.

5.1.6 Bearer Capability processing

The routing table offers the possibility to force the Bearer Capability Information Element for calls sent to the H.323 network or to the ISDN terminals.

The typical application is to force, for example, a "3.1Khz audio" bearer capability for a terminal which is not able to indicate this value (for example, for a voice-band modem).

If the Bearer Capability is forced to "Unrestricted", the call is then considered as a data call (the CES clear channel coding mode will be used).

5.1.7 Tones and Announcements

The OneOS-based voice-capable router generates a configurable dialing tone (on the B channel) in case of overlap dialing until the reception of the first digit.

The Information Element (IE) "progress in-band" can be passed on the ISDN ALERTING and CALL PROCEEDING messages. When such IE is passed, the ISDN B-Channel must be established so that the user can hear the ringback tone during call establishment.

The IE "progress in-band" is not passed transparently through the SIP signaling contrarily with H.323.

If the OneOS SIP gateway receives an 18x SIP response containing SDP (such "180 RINGING" or "183 Session In progress"), the SIP gateway builds the B-channel and starts listening to the RTP flow. In other words, when receiving SDP in 18x message, the SIP-gateway can connect the calling user to customized ringback tones.

If the OneOS SIP gateway receives the IE "progress in-band" on the ISDN side, the B-channel is open, the SIP gateway sends a SIP 183 response message and starts sending RTP. In that case, the ISDN terminal is providing a ringback tone or a special voice announcement.

5.1.8 Numbering plan management and Routing process

To make the routing table as simple as possible – routing the calls without handling the numbering plan prefixes (national, international, country code) –, OneOS can manage the numbering plan. The following functions are available for the routing process:

1. Apply a pre-processing or a dial plan to the calling and called numbers prior any routing process.
2. Apply the routing process (see the routing table configuration).
3. Apply call distribution (based on the priority of the port – load balancing).
4. Apply a post-processing to the calling and called numbers after the routing process.

5.1.9 Call-Triggered Reboot

It is possible, for maintenance purpose, to define a specific number to control a reboot. When a call is received with a configured specific number, the OneOS-based voice-capable router disconnects all the current calls and reboots. A specific configuration file that must be used after reboot can be indicated in the configuration (see the routing table configuration): the current startup configuration file is overwritten by the selected file.

This functionality can be used to reboot locally or remotely the device without entering in the configuration.

5.1.10 Date & Time

The OneOS-based voice-capable router can optionally send the date & time to the local ports (analog or ISDN) if it is synchronized on a SNTP/NTP server. This feature can be activated on a per-port basis (voice-port parameters).

5.1.11 Number Portability

During the transient phase when number portability between telephone operators is realized, the OneOS-based voice-capable router is also connected to the former ISDN network during a period to be sure that any call coming from the previous ISDN network is routed to the PBX and not lost. When the number portability is done, any call should be coming from the VoIP network so that the connection to the former ISDN network becomes useless.

A function, embedded in the OneOS-based voice-capable router, provides logs and alarms enabling a pro-active number portability management.

When the number portability is enabled, the OneOS-based voice-capable router starts in the "portability in-progress" state as soon a call is received from the VoIP network. A configurable timer is started. If a call is received on the ISDN network interfaces, the timer is restarted. If the timer is expired, the OneOS-based voice-capable router is in state "portability done". If the number portability is set to done and if a call is received on the interfaces connected to ISDN, then an alarm is generated.

An "alarm / event" is generated each time the state of number portability changes.

5.2 VOIP VOICE PROCESSING

With subscribers using ISDN, the voice signal coded in PCM 64Kbps (G.711 A-law or µ-law) from the subscriber side is either transmitted transparently or coded with a lower bit rate (e.g. G.729AB at 8Kbps) by the access device. The transit delay induced by the IP network can be higher than a few tens of milliseconds; consequently, the access device must cancel the electric echo generated by the 2-wire / 4-wire device inside the connected analog telephone terminals. In order to reduce the bandwidth requirement for voice communication, silence can be suppressed (based on VAD Voice Activity Detection).

These coders are supported:

- G.711 A law (64Kbps)
- G.711 µ-law (64Kbps)
- G.729A (8 Kbps, no silence suppression)
- G.729AB (8 kbps, with optional silence suppression)
- CES Clear Channel (64Kbps) for unrestricted data on ISDN interfaces (transparent codec)

The RTP/RTCP protocol is used for voice packet transmission.

The transmission periodicity is configurable at 10, 20, 30, 40 ms for G.729A/AB, G.711, and CES. The OneOS-based voice-capable router accepts any periodicity on the reception flow and supports the asymmetric coding mode (for example: transmission in G.729, reception in G.711).

The silence suppression is compliant with the standard referenced in G.729AB. For the other coders (G.711, G.726), silence is suppressed using an optional comfort noise generation (the noise level is sent periodically to the remote end) in conformance with RFC3389.

The CES enables the transmission of any data application over an ISDN B Channel. This coder is automatically selected if the Bearer Capability requested in the SETUP message indicates "unrestricted data" and if the local port is of ISDN type. For a reliable data communication without any error, the synchronization must be achieved externally and is identical for both sides of the communication:

- Synchronization provided by the ISDN port (if PRI or BRI in TE mode)
- Synchronization provided by the uplink if DSL is used.

5.2.1 Hosted Nat Traversal

In some applications, it is necessary to maintain a continuous RTP flow in order to keep the NAT sessions open in external routers. A parameter enables this feature: silence RTP packets are sent when the call is on hold as soon as the remote IP address & port are known. It is available for SIP only. See `rtp-permanent` parameter in `dial-peer voice voip` parameter group for more details.

5.2.2 Bandwidth Limitation

To avoid congestion on the uplink (and consequently a bad quality on each voice call), it can be necessary to have a bandwidth limitation.

It is possible to limit the total RTP bandwidth with a global parameter (sip/h323-gateway, `max-bandwidth` command). Upon each call, the current bandwidth is checked before accepting it. The voice coder list can be reduced to the low bit rate coders for this call if, for example, there is not enough bandwidth for G.711.

When several coders are available, OneOS allows using a better quality voice coder when the bandwidth is available (the preferred coder is G.711). If the bandwidth is available, the G.711 is selected for voice coding & decoding. In case of new call and if the actual used bandwidth is above a configured threshold of the available bandwidth (see `dynamic-coder-selection` command), then the coder of (one or more) current calls are switched from G.711 to G.729A (when a call is switched from G.711 to G.729A, there is no switch back to G.711). This feature is available in H.323 (capabilities renegotiation) and SIP (RE-INVITE). Calls are switched to G.729A according to the following rules:

- Pass through fax/modem calls, T38 fax calls and UDI64K calls are never switched to G.729A.

- Voice calls already switched to G.729A and switched back to G.711 by the remote end are switched to G.729A the last ones.
- Other voice calls are switched to G.729A the older first.

On selected OneOS-based voice-capable routers (see `g729-dynamic` command), it is possible for a better voice quality to use the G.729 codec instead of the G.729A codec when there is enough computing power. When there is not enough computing power (one or more) current calls are switched from G.729 to G.729A (when a call is switched from G.729 to G.729A, there is no switch back to G.729).

The number of concurrent calls can also be limited for each configured dial-peer VoIP.

In case of H.323, the bandwidth can also be controlled by the gatekeeper with the RAS signaling protocol (optional).

5.2.3 Emergency calls

The emergency call service gives highest priority to call destined to high priority dial numbers (such firefighter department). An emergency level is defined by a number between 1 and 200. A lower value has a higher emergency level or priority.

The process is the following:

1. An emergency level can be assigned to calls from defined local ports.
2. An emergency level can be assigned to a call by the routing process, depending on the called and/or the calling number.
3. The minimum value from cases #1 and #2 will be considered (for example, if physical port has an emergency level of 3 and the called number has an emergency level of 2, then the emergency level of the call will be 2).
4. When a call is routed to an interface and if there is not enough resources to send the call (no available B channel, bandwidth, etc...), the emergency level of the call is compared to the level of the current calls. If it is higher than a current level, the active call is disconnected and the resource is affected to the new call.

5.2.4 Group 3 FAX Processing

Transparent Mode

The G3 FAX can be transported by using G.711 coding. The OneOS-based voice-capable router automatically disables the Echo Canceller or switches the echo-canceller to a specific mode if a G3 FAX is detected (optional). The G.711 coder can be selected per configuration or dynamically during a voice communication when a modem or FAX is detected: this mode is called "Modem or FAX pass-through".

FAX Pass-through

The OneOS-based voice-capable router can switch to a G.711 coding mode dynamically during a voice communication when a Group 3 FAX is detected. The Echo Cancellation remains enabled but in a specific mode (NLP for G3 FAX). Several methods are proposed to force the communication to G.711:

- Direct mode: proprietary method consisting in switching the RTP flow to G.711 without any H.245 or SIP exchange.
- Request mode: standardized method using the H.245 "request-mode" message to force the closing of the current channels and the reopening of G.711 channels (H.323-specific).
- TCS Null method: the H.245 capabilities are renegotiated and forced to G.711 (H.323-specific).
- RE-INVITE method is used to renegotiate a coder compatible with fax pass-through (SIP-specific).

FAX Relay

The OneOS-based voice-capable router also supports FAX Relay compliant to ITU-T T.38 (UDP mode). The signal is modulated & demodulated locally, the T.30 messages are analyzed and relayed, and the fax data is transported transparently over IP/UDP. The V.27ter (4800 bps) and V.29 (9600 bps) modulations are supported. The OneOS-based voice-capable router offers FAX Spoofing to avoid FAX failures in case of long transit delay over IP. An optional mechanism forces a fallback of V34 FAX communication (Super G3) to Group 3 communication, so Super G3 faxes can communicate with T.38 instead of G.711 pass-through.

5.2.5 Modem Processing

Transparent Mode

A Modem signal can be transported by using G.711 coding mode. The OneOS-based voice-capable router can automatically disable the Echo Canceller if a modem is detected. The G.711 coder can be selected by configuration: permanently or on call-by-call basis by the calling/called number analysis.

Modem Pass-through

The OneOS-based voice-capable router can switch to a G.711 coding mode dynamically during a voice communication when a modem or Super Group 3 FAX is detected. The echo-cancellation is automatically disabled. Several methods are proposed to force the communication to G.711:

- Direct mode: proprietary method consisting in switching the RTP flow to G.711 without any H.245 or SIP message exchange.
- Request mode: standardized method using the H.245 "request-mode" message to force the closing of the current channels and the reopen of G.711 channels (H.323-specific).
- TCS Null method: the H.245 capabilities are renegotiated and forced to G.711 (H.323-specific).
- RE-INVITE method is used to renegotiate a coder (SIP-specific).

5.2.6 Echo Processing and Pass-through modes

Refer to the table on page 6.2-37 for more information.

5.2.7 DTMF Processing

DTMF is processed by using the H.245 message or via SIP INFO in alphanumeric format. The DTMF codes are detected in the received voice signal, suppressed before sending the RTP flow and regenerated at the remote end. The DTMF level and duration are configurable; however, the DTMF codes can be transmitted transparently when the G.711 coder is used.

Alternatively, DTMF can be processed in-band as specified by RFC 2833.

Note: SIP INFO method is not supported for DTMF coming from a remote SIP device.

5.2.8 MOS scoring

As of OneOS V4.2R4 software release, the Mean Opinion Score Conversational Quality (MOS-CQ) and the Mean Opinion Score Listening Quality (MOS-LQ) are included in the call detail records and statistics.

The MOS is a measurement (value between 1 and 5) of voice quality based on subjective criteria while surveying many people; the higher the MOS, the higher the probability a human being would consider voice quality to be excellent. Some models were created to compute a MOS evaluation from measurable data. One of them is the E-model of ITU-T Recommendation G.107. The E-model computes first an R factor; then a formula derives a MOS from R. The computation of R factor is complex and requires some metrics that cannot be easily obtained by OneOS. Some metrics have been then chosen to a default value.

The following table gives the definitions of the categories of speech transmission quality in terms of ranges of Transmission Rating Factor R provided by ITU-T Recommendation G.107. This table also gives the descriptions of "User satisfaction" and equivalent transformed values of R into conversional MOS-CQ for each category:

R-value (lower limit)	MOS-CQ	Speech transmission quality	User satisfaction
90	4.34	Best	Very satisfied
80	4.03	High	Satisfied
70	3.60	Medium	Some users dissatisfied
60	3.10	Low	Many users dissatisfied
50	2.58	Poor	Nearly all users dissatisfied

The MOS calculation is implementation dependant. The MOS reported by an OneOS-based voice-capable router must only be compared with another OneOS-based router, not with 3-rd party vendor. Under ideal conditions, OneOS returns a MOS-CQ of 4.00 for G.729A and 4.35 for G.711A.

The R factor for MOS-LQ calculation provided by OneOS takes into account the following parameters:

- End-to-end frame loss (not only RTP packets lost by the network, but also frames lost internally by OneOS DSP because the de-jitter buffer is full for example).
- Packet loss burstiness: packet loss concealment in DSP makes up for very sporadic packet loss so that a human ear hardly perceives the difference. But, if packet loss is bursty (i.e. 5 packets lost in a row), the impact on voice quality is worse.
- Network jitter.
- Codec type and packetization delay.

The R factor for MOS-CQ calculation takes into account the following additional parameters:

- Echo path loss and echo loudness rating.
- One-way delay: approximated via the formula `Ta = DSP_FIFO_Size + Round_Trip_Delay / 2`

The R factor calculation uses the information included in the RTCP and RTCP-XR frames received from the remote end. As of V4.2R4 software release, RTCP-XR is enabled by default. Prior to that release, RTCP-XR is disabled by default; in that case, make sure that RTCP-XR is enabled using the `rtcp-xr` command for a more accurate MOS calculation.

The MOS-CQ and MOS-LQ as well as the remote MOS-CQ and MOS-LQ are displayed on a call by call basis using the `show voice rtpcall short` command. The remote MOS-CQ and MOS-LQ are only available if the call duration is long enough for the RTP protocol to set-up and `rtcp-xr` is in force.

The graphical representation over time of the R factor related to MOS-CQ can be displayed on a call by call basis using the `show voice rtpcall full` command. The value of R is given every minute for the last 30 minutes of the call.

A mean value of MOS-CQ for all calls is calculated on the flow and can be displayed using the `show voice mos` command. Use the `show voice mos reset` command to restart the mean calculation.

6 VOIP CONFIGURATION

6.1 INTRODUCTION TO VOIP CONFIGURATION

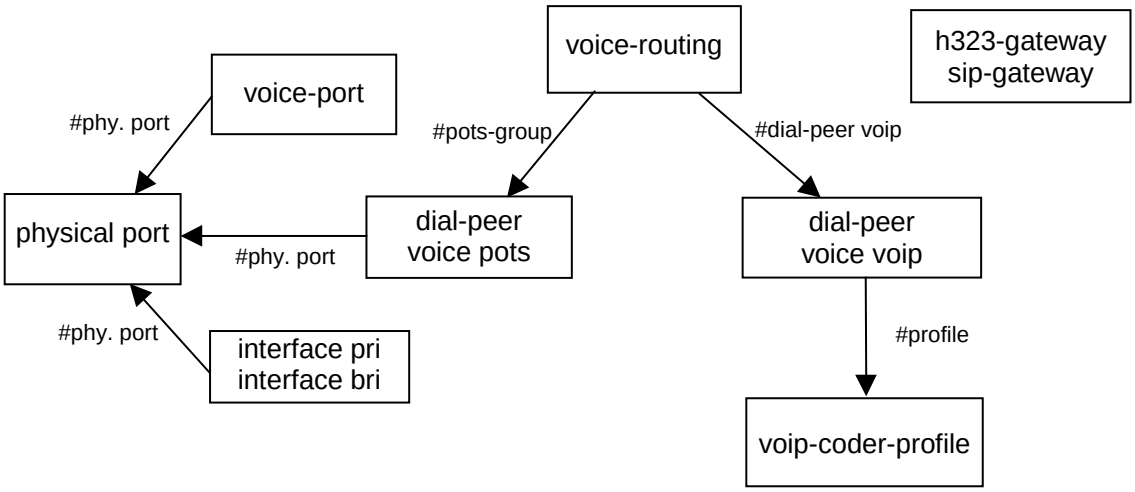
A set of command lines (CLI), dedicated to voice services enables the configuration of all necessary parameters. In general, the VoIP function requires the configuration of very few parameters. The OneOS-based voice-capable router permits the configuration of a comprehensive parameter set in order to adapt to all cases described in the standards. Most parameters will be set with default values, thereby reducing the number of steps required to configure the device.

6.1.1 Configuration Items

The configuration includes the following main commands:

- `voice-port`: physical BRI/PRI/E1R2/FXS/FXO port. Voice processing parameters are defined such as echo cancellation, gain and coding law.
- `interface`: defines, for BRI/PRI/E1R2 only, parameters for the physical layer and ISDN protocol.
- `dial-peer voice`: logical internal ports (see below `dial-peer voice pots` and `voip`).
- `dial-peer voice pots`: local voice port always associated with a physical port (i.e. BRI/PRI/FXS/FXO port). It enables the configuration of groups, direct call and number transformation.
- `dial-peer voice voip`: remote H.323/SIP device. The IP address, H.323/SIP protocol parameters and coder profile are defined here. If a gatekeeper/registrar is used and all the remote devices have the same H.323/SIP parameters, a single `dial-peer voip` can be configured.
- `voip-coder-profile`: to define a list of coders to be negotiated during capabilities exchange.
- `SIP/H323-gateway`: defines all the parameters related to the SIP/H.323 gateway (use of gatekeeper/registrar, protocol parameters).
- `voice-routing`: defines the rules to route the calls between the dial-peers (`pots` and `voip`).

The relationships between configuration items are described in the following diagram:



The following sequence for configuration is preferred:

1. The physical voice ports using the `voice-port` command (see 6.2).
2. The PRI or BRI interfaces using the `interface pri` and/or `interface bri` commands (see 6.3).
3. The E1 R2 interface using the `cas-r2` command (see 6.4).
4. The local voice ports using the `dial-peer voice pots` command (see 6.5).
5. The voice gateway using the `h323-gateway` or `sip-gateway` command ***(Note that H.323 and SIP are not supported simultaneously)*** (see 6.6 or 6.7 respectively).
6. The voice coder profiles using the `voip-coder-profile` command (see 6.8).
7. The remote voice devices using the `dial-peer voice voip` command (see 6.9).
8. °The voice calls routing using the `voice-routing` command (see 7).

6.1.2 Configuration Management

All the parameters may be changed online, except a few parameters specified in SIP/H.323-gateway. For these parameters, a shutdown command of the SIP/H.323 gateway is required (this requirement is indicated by a warning message).

6.2 VOIP: PHYSICAL VOICE PORTS CONFIGURATION

The OneOS-based voice-capable router voice module is always designated by the number 5. The physical port is identified with a port number in the [0..(n-1)] range, where n is the total port number of the interface module (currently up to 13).

Command for creation of physical port number 0 (voice module number is 5):

```
CLI(configure)> voice-port 5/0
CLI(voice-port)>
```

6.2.1 Common parameters

The parameters in this chapter are common to analog (FXS/FXO), ISDN (BRI/PRI) and E1R2 physical ports.

6.2.1.1 Parameters for Echo Cancellation

To enable the echo canceller – default: enabled –, use the following command. Use the `no` form of the command to disable the echo cancellation.

```
CLI(voice-port)> [no] echo-cancellation
```

To define the maximum tail length, use the following command. The `low` value is 8ms, `medium` is 16ms – default –, `high` is 32 ms; it must be configured `medium` or `high` if off-net calls must be supported.

```
CLI(voice-port)> echo-cancellation-length { low | medium | high }
```

On ONE300, when using G.729 codec, 30 voice channels can only be supported if echo-cancellation low or medium is selected.

To specify the conditions for automatically disabling the echo canceller on FAX or modem detection, use the following command. Default: no echo disabling. See the table below for parameter description.

```
CLI(voice-port)> [no] echo-disable { voicemodem | modem }
```

Note: `voicemodem` should be used only in particular cases when it is needed to disable only the non-linear processor of the echo canceller to make low speed faxes and modems work properly (especially with noisy or low level signals).

The following table summarizes the actions taken when detecting a FAX or a modem taking into account the echo disabling (at voice port level) and pass-through modes parameters (at dial peer VoIP level).

Note that there are other fax-relay modes than pass-through (please refer to 6.9.1).

CLI configuration	action on CED tone detected (1)	action on ANS or ANSam tone detected (2)
no echo-disable no modem-passthrough no fax-relay passthrough	no action taken	no action taken
echo-disable voicemodem no modem-passthrough no fax-relay passthrough	disable NLP part of echo canceller disable DTMF detection disable VAD	disable echo canceller disable DTMF detection disable VAD
echo-disable modem no modem-passthrough no fax-relay passthrough	disable echo canceller disable DTMF detection disable VAD	disable echo canceller disable DTMF detection disable VAD

CLI configuration	action on CED tone detected (1)	action on ANS or ANSam tone detected (2)
modem-passthrough no fax-relay passthrough	disable echo canceller (3) disable DTMF detection (3) disable VAD (3) switch to G.711 coder (3)	disable echo canceller disable DTMF detection disable VAD switch to G.711 coder
fax-relay passthrough no modem-passthrough	disable NLP part of echo canceller (4) or disable echo canceller (4) disable DTMF detection disable VAD switch to G.711 coder	no action taken
fax-relay passthrough **modem-passthrough**	disable NLP part of echo canceller (4) or disable echo canceller (4) disable DTMF detection disable VAD switch to G.711 coder	disable echo canceller disable DTMF detection disable VAD switch to G.711 coder

(1): CED tone is used by Group 3 (G3) faxes and low speed modems up to V.29 modulation (9600 bps). G3 fax detection is done according to `detection-fax` configuration (V.21 or CED).

(2): ANS or ANSam tone is used by Super Group 3 (SG3) faxes and high speed modems (from V.32 modulation and above)

(3): in that case G3 faxes are considered as low speed modems

(4): according to `echo-disable` configuration

6.2.1.2 Parameters for Gain control

To define the output gain (dB) and amplify the signal for the voice flow sent to the remote VoIP peer – device connected to voice port (e.g.: PABX or telephone set) –, use the following command:

```
CLI(voice-port)> output-gain <gain: -12..+12 dBm; default: 0 no gain>
```

To define the input gain (dB) and amplify the signal for the voice flow received from the remote VoIP peer – device connected to voice port (e.g.: PABX or telephone set) –, use the following command:

```
CLI(voice-port)> input-gain <gain: -12..+12 dBm; default: 0 no gain>
```

6.2.1.3 Parameters for Synchronization

To select the synchronization input – default: `free_run` –, use the following command:

```
CLI(voice-port)> clock-source { free_run | uplink | bri | pri | rtp }
[<period>] [priority <0-255>] [fallback { free_run | rtp }]
```

As a unique clock source must be used in the device, the modification is automatically applied to all relevant voice-ports.

If `free-run` is selected, the internal clock is used and the command is automatically applied to all voice-ports.

If `uplink` is selected, the clock is retrieved from the uplink interface and the command is automatically applied to all voice-ports.

If `bri` is selected, any BRI interface (that must be configured as TE for the physical layer) with the layer 1 activated is automatically selected for the clock synchronization. If there is no BRI interface in TE mode with layer 1 activated, the internal clock is used (`free_run`). The command is automatically applied to all BRI ports.

If `pri` is selected, it must be configured on the PRI interface used for synchronization. In case of a two-PRI device, one PRI can be selected to be "slave" and the other one "master" in terms of clocking.

If `rtp` is used, the clock is retrieved from the RTP flow (refer to 12) and the command is automatically applied to all voice-ports.

The `period` parameter and the `priority` parameter are not used; they can be omitted.

The `fallback` parameter defines which clock is used when the configured clock is not available. It can be either the RTP clock (`rtp`) or the internal clock (`free_run`).

6.2.1.4 Parameters for Tones

The following command specifies the tones signal parameters. The frequencies and durations used comply with the selected country specifications (default France).

```
CLI(voice-port)> tone { Australia | Austria | Belgium | CzechRepublic
                      | Denmark | France | Germany | Ireland | IrelandUK
                      | Italy | Netherlands | NewZealand | Portugal
                      | Spain | Sweden | Switzerland | UK | USA
                      | userdefined }
```

The following command specifies the transmit level for tones (dBm). Default: -10 dBm.

```
CLI(voice-port)> tone-level <-40 to 0>
```

The following command can be used, after having selected a country, to modify the characteristics of one or more tones if needed.

```
CLI(voice-port)> modify-tone { dial | network-failure | congestion | busy
                             | ring-back | callback | mwi | cwi | other
                             | special-info | special-conf | special-dial
                             } <new-tone-specs-string>
```

`busy` tone is used to tell the caller that the called party is already in communication.

`congestion` tone is used to tell the caller that the communication has failed because of congestion in the network.

`callback` tone is used to tell the caller that the called station is ringing (incoming call indication).

`cwi` (Call Waiting Indicator) tone is used to alert a party using the phone to an incoming second call.

`dial` tone is used to indicate that a number may be dialed.

`mwi` (Message Waiting Indicator) tone is used to indicate the presence of information of the messaging service (voice-mail).

`network-failure` tone is used to indicate that the call is terminated (release of the call).

`other` tone is not used.

`special-info` tone is used to indicate that call forwarding (CFX) is enabled or disabled successfully. It is also used as a positive response to a question about call forwarding.

`special-conf` tone is used in negative answer to a question about call forwarding (CFX).

`special-dial` tone is the dialing tone used when call forwarding (CFX) is active.

The specifications of the new tone are given in the string `new-tone-specs-string` (up to 127 characters) made of two parts separated by a semicolon character (**;**).

- The first part describes the various clean frequencies (up to 6) that compose the tone. Each frequency description is a field of the form `frequency in Hz@level in dBm`. The frequency fields are separated by commas (**,**). They are implicitly numbered from 1 up to 6 as they appear.
- The last part describes the tone over time. It is made of one duration field (in seconds) followed, between parentheses, by the cadences (up to 6) that make the tone. Each cadence description is a field of the form `time on in seconds/time off in seconds/frequency number(s)`. Within the parentheses, the cadence fields are separated by commas (**,**). Several clean frequencies can be used in one cadence; in that case the numbers are separated by plus (+). Silence is the frequency number 0. An always on frequency has star (*****) as on time and 0 as off time.

Examples:

- `350@-19,440@-19;10(*/0/1+2)` for a 10-second tone made of 350Hz+440Hz at -19dBm (always on/never off/frequencies 1 and 2), default dial tone (USA).

- 985@-16,1428@-16,1777@-16;20(.380/0/1,.380/0/2,.380/0/3,0/4/0) for a 20-second tone made of 380ms of 985Hz at -16dBm followed by 380ms of 1428Hz at -16dBm followed by 380ms of 1777Hz at -16dBm followed by 4 seconds of silence, special information tone SIT1 (USA).

The following commands are deprecated and replaced by the above defined command.

```
CLI(voice-port)> tone userdefined
CLI(voice-port)> user-tone …
CLI(user-tone)> timing …
CLI(user-tone)> frequency …
```

6.2.1.5 Parameters for Dialing

The following command defines the maximum time (in seconds) for receiving the first digit. Default: 10sec.

```
CLI(voice-port)> dialing-timer <1-30 seconds>
```

The following command defines the idle time (first timer) without receiving a digit to consider the dialing completed when `timer` or `timer-or-#` is selected in the routing table. Default: 4sec. Also, this command optionally defines the idle time (second timer) without receiving a digit to consider the dialing completed when partial match is used in the routing table (in that case the routing process exits the route with partial match when the second timer elapses and continues with other routes). Default: 10sec.

```
CLI(voice-port)> end-of-dialing-timer <1-30 sec> [<1-30 sec>]
```

The following command enables the second step dialing mode for FXO port only. Default: disable, which means incoming dialed digits are processed through the voice routing table. If enabled, the FXO interface accepts any incoming call and works as a FXS port for receiving DTMF dialing.

```
CLI(voice-port)> second-step-dialing { enable | disable }
```

The following command specifies the time between off-hook and the transmission of the first digit for FXO interface. Default: 2sec.

```
CLI(voice-port)> timeout-before-dialing <1-60 sec>
```

The following command defines the transmitted DTMF digit duration. Default: 100ms.

```
CLI(voice-port)> digit-duration <50-1000 ms>
```

The following command defines the minimum delay between two DTMF digits (for transmission towards the terminal). Default: 100ms.

```
CLI(voice-port)> inter-digit <50-1000 ms>
```

The following command configures the criterion level for DTMF detection. `normal` (default) is a good compromise between DTMF detection on one hand and voice detection on the other hand, without degrading highly the real time performance. `severe` can be used in some cases when it might happen that some fragment of voice talks are interpreted as DTMF. `large` can be used in some other cases when it might happen that some DTMF digits are missing.

```
CLI(voice-port)> dtmf-detection-criterion { normal | severe | large }
```

6.2.1.6 Parameters for Advice of Charge

The following parameters in this section can be not valid if the softswitch does not support them.

To configure the Advice of Charge "D" (during the call) information, use the following command. Use the `forced` parameter to force the AOC-D request for any call received on a voice port (analog or ISDN). Use the `transparent` parameter to make the AOC-D request being forwarded. Use the `no` form of the command to disable the AOC-D and have the request being discarded. Default: disabled (no).

```
CLI(voice-port)> [no] aoc-d-service { transparent | forced }
```

To configure the Advice of Charge "E" (end of call) information, use the following command. Use the `forced` parameter to force the AOC-E request for any call received on a voice port (analog or ISDN). Use the `transparent` parameter to make the AOC-E request being forwarded. Use the `no` form of the command to disable the AOC-E and have the request being discarded. Default: disabled (no).

```
CLI(voice-port)> [no] aoc-e-service { transparent | forced }
```

6.2.1.7 Miscellaneous Parameters

Use the following command to enable or disable the presentation of the name if the information is available from the VoIP call leg. When disabled, the name is not presented. Default: enable.

```
CLI(voice-port)> calling-name-presentation { enable | disable }
```

Use the following command to enable a loop mode on B channel or FXS while the call is connected. This feature is commonly used for hardware testing. Default: `no loop`.

```
CLI(voice-port)> [no] loop
```

Date and time is sent to local port (analog or ISDN) if the OneOS-based router is connected to a NTP server. On ISDN, the date/time is provided in CONNECT message in IE 29. In other words, ***you need to place a successful call from ISDN*** in order to have the time/date of ISDN phone updated.

```
CLI(voice-port)> sntp-time
```

Use the following command to enable, if the voice port is in "no shutdown" state, the operational state of the port to be taken into account for the state of the front panel "voice" LED. Use the no form to disable the process. Default: enable.

```
CLI(voice-port)> [no] led-alarm-report
```

Use the following command to enable the lifeline bypass if the voice service is not ready (not registered to a Gatekeeper or Registrar or call-agent). This parameter is also present in interface BRI parameter group. Use the no form to disable the lifeline bypass. Default: disable.

```
CLI(voice-port)> [no] life-line-hold
```

Use the following command to display the life-line status.

```
CLI> show voice life-line
```

6.2.2 ISDN ports specific parameters

6.2.2.1 Parameters for Power Source One (ISDN ports only)

To enable (disable) the power source one (PS1) on the BRI interfaces – default enabled –, use the following command. It is global for all the ports: any modification is automatically applied to all the voice ports.

```
CLI(voice-port)> [no] power-source-one
```

6.2.2.2 Parameters for Tones (ISDN ports only)

If configured, the following parameter enables the local generation of a ringback/callback tone in the B channel (this command is a workaround for certain bad H.323 implementation in softswitch/media-gateways, - only for H.323 -).

```
CLI(voice-port)> [no] isdn-ringback-tone
```

When an ISDN subscriber is called, some PBX/phone includes the option "Progress-in-Band" in ALERTING message. This has the effect of connecting the B-channel. It is expected that the PBX/ISDN phone generates then the ringback tone. Some ISDN phones/PBXs do not. To make up for such bad behavior, the OneOS-based voice-capable router can add the local ringback tone to the RTP stream, so that the remote party finally hears ringback tone in reverse direction (hence "reverse-ringback-tone"). The following parameter must NOT be entered as default because the ISDN/PBX ringback signal would be added to the local ringback.

```
CLI(voice-port)> [no] isdn-reverse-ringback-tone
```

If configured, the following parameter enables the local generation of release tone (network-failure, congestion, busy) in the B-channel and the IE "Progress-in-Band" is inserted in ISDN DISCONNECT message. This feature is needed for certain PBXs that never generate the release ringback tone.

```
CLI(voice-port)> [no] isdn-release-tone
```

The following command includes the IE "Progress-in-Band" in SETUP-ACK sent by the OneOS-based router. This IE may be needed by certain ISDN phone to connect the B-channel and receive the dial-tone from the router.

```
CLI(voice-port)> [no] isdn-setupack-inband
```

6.2.2.3 Parameters for User-to-User Service (ISDN ports only)

Use the following command to select the type of user-to-user service (UUS) supported by the port. When a specific service is not configured, UUS Information Elements are stripped from the ISDN message before forwarding process (default: service 1 – UUS1):

```
CLI(voice-port)> ie-uui [service { 1 | 2 | 3 | 1&2 | 1&3 | 2&3 | 1to3 }]
```

6.2.2.4 Parameters for Call Forwarding Service (ISDN ports only)

The following parameters allow discarding some service requests coming from the ISDN terminal: invocations of call forwarding (CFU, CFB, CFNR, and CCBS), call deflection (CD) and call rerouting.

```
CLI(voice-port)> no isdn-call-forwarding

CLI(voice-port)> no isdn-call-deflection

CLI(voice-port)> no isdn-call-rerouting
```

The ISDN call forward invocation (CFU, CFB, and CFNR) is saved by OneOS. A file in flash memory contains the phone numbers that requested the CFx service. When the CFx state is saved in OneOS, OneOS takes the decision that a call must be forwarded or not when receiving an inbound INVITE destined to a number that requested CFx. If OneOS takes the decision to forward the call, OneOS replies with the SIP response code "302 Moved" to the caller. The call should be then diverted by the network.

It is possible to activate and/or deactivate ISDN Call Forwarding Unconditional (CFU), Call Forwarding Non Response (CFNR) and Call Forwarding Busy (CFB) services by setting the following command:

```
CLI(voice-port)> cfx-command { activation | deactivation }
                             { cfu | cfb | cfnr }
                             <service> <SrvTypeOfNumber> <SrvNumber>
                             [<FwdTypeOfNumber> <FwdNumber>]
```

service: **{ speech | unrestr-digit | audio_3k1hz | unrestr-digit-tone**
| telephony_3k1hz | teletex | telefax_g4 | videotex
| video | telefax_g2_3 | telephony_7Khz | all }

SrvTypeOfNumber is the served type of number: **{ none | public_unkown**
| public_international | public_national | public_networkspec
| public_subscribed | public_abbreviated | private_unkown | private_level2
| private_level1 | private_networkspec | private_local | private_abbreviated }

SrvNumber is the served number [(35 digits max) **[0-9,*,#]** or allNumbers]

FwdTypeOfNumber is the forwarded type of number: **{ none | public_unkown**
| public_international | public_national | public_networkspec
| public_subscribed | public_abbreviated | private_unkown | private_level2
| private_level1 | private_networkspec | private_local | private_abbreviated }

FwdNumber is the forwarded number [(35 digits max) **[0-9,*,#] or** allNumbers**]**

Remarks:

- FwdTypeOfNumber & FwdNumber parameters are mandatory when activation command is set and ignored for deactivation command.
- These commands are not saved into the configuration file.

Example:

```
CLI(configure)> voice-port 5/1
CLI(voice-port)> cfx-command activation cfu speech public_international
2409995773 public_national 2409995779
00:15:24.121 Info vox voip controlplan 3 Diversion activation configured
by user on local port: 5/1
00:15:24.179 Info vox voip controlplan 3 Diversion activation action
successful.
```

The CFx state can be viewed by means of the following command:

```
CLI> show voice cfx { <voice_port:5/x> | all }
```

Example:

```
CLI> show voice cfx all
<1>
Line               = 5/1
Type               = Unconditional (CFU) ACT
basicService       = 0x02 (speech)
forwardedTypeOfNb  = public,national
forwardedToAddress = 2409995779
ServedTypeOfNb     = public,international
ServedAddress      = 2409995773

>>> 1 records.
```

To remove the saved CFx state:

```
CLI> show voice cfx { <voice_port:5/x> | all } reset
```

6.2.3 Analog ports specific parameters

6.2.3.1 Parameters for ringing (analog ports only)

For analog ports only, the following command specifies the ring signal parameters. The frequency used complies with the selected country specifications. Default: France.

```
CLI(voice-port)> ring { Australia | Austria | Belgium | Denmark | France
                      | Germany | Ireland | IrelandUK | Italy
                      | Netherlands | Portugal | Spain | Sweden
                      | Switzerland | UK | USA | userdefined }
```

The following command defines the ringing parameters for the `userdefined` ringing profile. `freq` is the frequency from 0 to 60 Hz, `ton` / `toff` are the emission/pause durations in ms (0-5000).

```
CLI(voice-port)> [no] user-ring <freq> <ton-1> <toff-1> <ton-2> <toff-2>
```

The following command specifies the standard to use to send the caller ID. Default: none. If FSK is selected, the caller ID as well as the time/date of the OneOS-based router is passed to the FXS phone.

```
CLI(voice-port)> caller-id { none | dtmf | fsk }
```

The following command specifies the initial ring tone (ms) for caller-id.

```
CLI(voice-port)> initial-ring <10-2000>
```

The following command defines the ringing voltage, for analog ports only (default: normal).

```
CLI(voice-port)> ring-level { normal | min | high | max }
```

The following table gives the available ring levels (values are for 2 REN ETSI).

ring level	FXS150 board	FXS300 board	other FXS boards
normal	37.5 Vrms centered on 45Vdc	37.5 Vrms centered on 41Vdc	37.5 Vrms centered on 22Vdc
min	40 Vrms centered on 37Vdc	40 Vrms centered on 37Vdc	40 Vrms centered on 18Vdc
high	52 Vrms centered on 25Vdc	52 Vrms centered on 22Vdc	40 Vrms centered on 18Vdc
max	65 Vrms centered on 8Vdc	65 Vrms centered on 0Vdc	45 Vrms centered on 11Vdc

The following command defines the timeout for incoming call on FXO ports: after receiving a ringing signal, the call is disconnected if no ringing signal is received anymore during this time. Default: 6 sec.

```
CLI(voice-port)> fxo-ringing-timeout <1–30sec>
```

The following command defines the maximum time for ringing without detecting off-hook. Default: 120sec. This command applies only to FXS ports. For ISDN ports please use the T301 timer.

```
CLI(voice-port)> max-ringing <1-180 sec>
```

The following command defines the number of pulse for ringing signal detection on FXO port. Default: 2.

```
CLI(voice-port)> ring-number <1-40 pulses>
```

6.2.3.2 Parameters for Loop State management (analog ports only)

Use the following command to specify the minimum duration (ms) of the "on-hook" state between two successive calls (FXO interface only). Default: 500 ms.

```
CLI(voice-port)> on-hook-min-duration <20..10000 ms>
```

Use the following command to enable the polarity inversion for FXS ports: the line power polarity is inverted upon the call connection. Use the no form to disable the polarity inversion. Default: disable.

```
CLI(voice-port)> [no] polarity-inversion
```

6.2.3.3 Parameters for Country-specific Characteristics (analog ports only)

Use the following command to change the timing parameters for the signals, which must be analyzed on FXS interfaces.

```
CLI(voice-port)> sig-conf {on-hook | off-hook | ring | flash |pulse-dial}
          <state1>/<duration1>,<state2>/<duration2>[,<state3/duration3>]
          [<tolerance 10..90>]
```

Three successive states can be defined:

`state` value 0 is used for "disconnected loop", value 1 for "connected loop" with a specific `duration`: in ms, from 1 to 10000 ms and `tolerance`: in % (default 30).

Warning: with large tolerance value, a signal (e.g. flash) could be interpreted as another signal (e.g. off-hook or on-hook).

Example: `sig-conf on-hook 1/10,0/400 70`. The On-hook signal will be validated if the OneOS-based voice-capable router detects a stable "connected loop" state during 10ms (+ or – 70%) and a stable "disconnected loop" during 400ms (+ or – 70%).

Example: pulse-dial for old dial-button telephones: `0/70,1/35 40`.

Default values: On-hook: `1/2,0/500 30`
Off-hook: `0/2,1/80 30`
Hook flash: `1/2,0/240,1/200 30`
Ring: obsolete
Pulse-dial: `0/50,1/50 30`

Use the following command to define the impedance type for FXS/FXO interface. All impedance types are available for FXO ports; only the four following impedance types (zetsi, 600, zbt3 and ztn12) are available for FXS ports.

```
CLI(voice-port)> impedance { zetsi | 600 | zbt3 | 600r | 600c | 900r
| 900c | complex1 | complex2 | complex3 | complex4 | complex5 | complex6
| complex7 | complex8 | complex9 | complex10 | complex11 | complex12 }
```

- zetsi: compliant with ETSI requirements (= complex2, default value)
- 600: 600 ohms
- zbt3: compliant with BT3 requirements (= complex3)
- 600r: 600 ohms
- 600c: 600 ohms + 2.16 µF
- 900r: 900 ohms
- 900c: 900 ohms + 2.16 µF
- complex1 also ztn12: 220 ohms + (820 ohms || 120 nF) and 220 ohms + (820 ohms || 115 nF)
- complex2: 270 ohms + (750 ohms || 150 nF) and 275 ohms + (780 ohms || 150 nF)
- complex3: 370 ohms + (620 ohms || 310 nF)
- complex4: 370 ohms + (820 ohms || 110 nF)
- complex5: 370 ohms + (1050 ohms || 230 nF)
- complex6: 350 ohms + (1000 ohms || 210 nF)
- complex7: 275 ohms + (780 ohms || 115 nF)
- complex8: 120 ohms + (820 ohms || 110 nF)
- complex9: 200 ohms + (680 ohms || 100 nF)
- complex10: 900 ohms + 1 µF
- complex11: 600 ohms + 1 µF
- complex12: global complex impedance (can be used when impedance specification is not known)

Use the following command to define other FXO parameters (than impedance) related to the country specifications. Note that other countries are available (refer to the help of the command).

```
CLI(voice-port)> fxo-country { Australia | Austria | Belgium | Denmark
| France | Germany | Ireland | Italy | Netherlands | Portugal | Spain
| Sweden | Switzerland | UK | USA }
```

6.2.3.4 Parameters for FXS Line Power Drop (analog ports only)

The following command configures the timer used for the FXS power drop feature:

```
CLI(voice-port)> fxs-power-timeout init <hh:mm:ss> down <hh:mm:ss>
                                                   up <hh:mm:ss>
```

init: the power is up at the device starting and this timer is started. If the VoIP gateway is not operational when this timer expires, the power is dropped. Default: 180sec.

down: if the VoIP gateway is not operational during this time, the power is dropped. Default: 60sec.

up: if the VoIP gateway becomes operational during this time, the power is switched on. Default: 60sec.

The up and down timers are defined to avoid power on/off in case of unstable VoIP gateway state. The init timer replaces the down timer for the device starting phase (after a reboot, it may take a long time to have the VoIP gateway up).

6.2.3.5 Parameters for Analog MWI (analog ports only)

The MWI service indicates on a phone LED or display if there are messages waiting in voice mail box.

```
CLI(voice-port)> analog-mwi { disable | enabled }
     [on-hook-only | specific-tone-only] [notification | transition]
     [date-time | message-id | calling-type | visual-ind | num-msg | all]
```

Default value: enabled on-hook-only notification all

If enabled (default value), the MWI is provided, in on-hook state by a short ringing signal followed by a modulated signal; in off-hook state by a modulated signal and with a specific tone instead of the dial tone. It is possible to enable one of these actions only. `on-hook-only`: the MWI is provided only in the on-hook state (default value). `specific-tone-only`: the MWI is provided only upon an off-hook event instead of the dial tone (if there is at least one message leaving in the mailbox). See table below.

Use the `notification` mode (default value) to send MWI information when receiving SIP NOTIFY message containing MWI information. Use the `transition` mode to start MWI information when receiving SIP NOTIFY message containing MWI information and when MWI transition (between the state "no message" and the state "at least one message") occurs. This option is used in case of phones which are not able to filter the short ringing signal sent for MWI in the on-hook state.

Use the last parameter (default value: all) to define which elements (separated by commas) to add to the message so as to be displayed on the phone display.

CLI command \ voice-port status and tone	On-hook	Off-hook	Specific MWI dial-tone
Disable	NO	NO	NO
Enabled	YES	YES	YES
Enabled on-hook-only	YES	NO	YES
Enabled specific-tone-only	NO	NO	YES

When the SIP voice mail server is fully RFC compliant, the OneOS-based voice-capable router must issue a SUBSCRIBE request to voice mail server so that the voice mail server can send a NOTIFY message when voice mails are pending for reading. Under SIP gateway configuration, the following lines must be configured for SUBSCRIBE:

```
CLI(configure)> sip-gateway
CLI(sipgw)> [no] voicemail-dns-add <ip-or-hostname> [:<port>]
                                                    [via <ip-address>]
CLI(sipgw)> [no] subscription-duration <seconds>
```

When those two lines are configured, the OneOS-based voice-capable router scans the list of prefix in voice-routing and send a SUBSCRIBE for all prefix that are SIP phone numbers (i.e. prefix without wild cards and with the `ua-sip` attribute).

`via` is the address of an outbound proxy. Default subscription interval: 1800 seconds. The following timer can be also configured (time interval between SIP SUBSCRIBE requests when SUBSCRIBE is not positively acknowledged, default: 60 sec):

```
CLI(sipgw)> subscription-failed <seconds>
```

6.2.3.6 Parameters for Analog CLIP (analog ports only)

The CLIP service indicates on the phone display the information related to the caller identity. Use the optional parameter (default value: all) to define which elements (separated by commas) to add to the caller identity so as to be displayed on the phone display.

```
CLI(voice-port)> analog-clip-ie [display | date-time | calling-id
                              | called-id | calling-name | call-type | all]
```

Default value: `all`

The following parameter defines how the Advice of Charge information is send to the analog terminal on FXS port. Default: none.

```
CLI(voice-port)> analog-aoc-type { none | 12khz | 16khz | RP | etsi }
```

6.2.3.7 Parameter for Reverse Ringback Tone (analog ports only)

By default, when an analog subscriber is called, the OneOS-based voice-capable router adds the local ringback tone to the RTP stream, so that the remote party finally hears ringback tone in reverse direction (hence "reverse-ringback-tone"). The following parameter can be used to prevent adding the local ringback tone to the RTP stream.

```
CLI(voice-port)> no analog-reverse-ringback-tone
```

6.2.3.8 Parameter for Call-waiting duration (analog ports only)

By default, when an incoming call occurs on a FXS port that is already in a call (connected), the second call waits to be connected for 45 seconds before being released. The following parameter can be used to modify the call-waiting timer.

```
CLI(voice-port)> fxs-call-waiting-timer <1..180: default 45 seconds>
```

6.2.4 FXS Supplementary Services Parameters

6.2.4.1 Configuring FXS Voice Features

By default, an FXS line can manage only one SIP call. Advanced voice features can be provided by a softswitch, if the softswitch manages internally the voice features and especially the connection of this FXS line with multiple subscribers (hold, retrieve, conference …).

In order to be softswitch-independent, the FXS line can be configured to be "intelligent", which means call control intelligence is in OneOS. Per FXS line, we can manage two calls, where one call is active and the other is on-hold. If 3-way conference is started, the conference is realized in OneOS gateway. By default second call and 3-way conference are managed using R key followed by a number; use the `recall-only` parameter to manage these services using R key not followed by a number and on-hook.

To configure an FXS line in "intelligent" mode:

```
CLI(configure)> voice-port 5/<x>
CLI(voice-port)> analog-user-profile intelligent [recall-only]
```

To return to standard FXS line (non-intelligent; default value):

```
CLI(voice-port)> analog-user-profile non-intelligent
```

Use the following command to set the way explicit call transfer is made. In double call state, the user can either hook on or press hookflash (R key) and a number. Call transfer is active only if analog-user-profile is set to intelligent:

```
CLI(voice-port)> analog-ect on { on-hook | flash-<y> }
```

Use the following command to force the calling number header for the Call Line Identification Restriction complementary service. See 4.2.3.2 for permitted values. It is also possible to enable this feature in the voice routing table.

```
CLI(voice-port)> force-clir <presentation-code> <screening-code>
```

Use the following command to configure the profile which defines the keypad sequence for Call forwarding (CFU, CFB, and CFNR).

```
CLI(voice-port)> [no] dialed-supp-service-profile <0..4>
```

For every call forwarding type, 3 keypads must be defined: one for activation, one for de-activation, one for checking (interrogating) the call forward status). The profile is defined in the voice-global parameter group:

```
CLI(configure)> voice-global
CLI(voice-global)> [no] dialed-supp-service-profile <0..4>
CLI(service-profile> [no] cfu activation <string> deactivation <string>
                                                  checking <string>
CLI(service-profile> [no] cfb activation <string> deactivation <string>
                                                  checking <string>
CLI(service-profile> [no] cfnr activation <string> deactivation <string>
                                                  checking <string>
CLI(service-profile> exit
CLI(voice-global)> exit
CLI(configure)> exit
```

The `string` must be not routable in the voice-routing table; a check is done while the CLI command is entered.

Example: `cfb activation *55# deactivation *55* checking #55#`

When the analog-user-profile is set to intelligent, the 3-pty conference can be managed internally or externally.

```
CLI(configure)> voice-port 5/<x>
CLI(voice-port)> 3pty-service { internal | external bridge-number
                                                    <bridge-phone-number>}
CLI(voice-port)> exit
```

Should the conference be managed in an external bridge, the 3pty service must be configured as follows:

```
CLI(configure)> sip-gateway
CLI(sipgw)> [no] bridge-uri-host <hostname-or-ip>
```

`bridge-phone-number` is the number included in request URI and "To" field. `hostname-or-ip` is the hostname or IP for INVITE request URI/"To" ("To" field is bridge-phone-number@hostname-or-ip).

3-way conference with an external bridge works as follows:

- The FXS subscriber must be connected to two other SIP subscribers (user B and C) where one call leg is on-hold.
- The FXS subscriber decides to activate 3-way conference and dials R3.
- OneOS initiate a first call to the conference bridge (a simple call to the bridge-phone-number).
- FXS is connected with the audio stream from/to this conference bridge and sends a REFER to user B and C so that B and C connects to the conference bridge.

Note that 3-way conference is possible to an OneOS-based voice-capable router as well as a SIP/H.323 conference bridge. The OneOS Conference Bridge is a `dial-peer voice pots` with the attribute `service voice-bridge`. When multiple subscriber call this dial-peer, the calls are accepted and the voice signals are mixed (up to `max-call` are accepted). To configure an OneOS Conference Bridge:

```
CLI(configure)> dial-peer voice pots <x>
CLI(pots)> pots-group <y>
CLI(pots)> service voice-bridge <max-call>
CLI(pots)> no shutdown
CLI(pots)> exit
CLI(configure)> voice-routing
CLI(voice-route)> route <route>
CLI(voice-route)> prefix <conf-bridge-number> length <len>
CLI(conf-voice-route)> dial-peer pots-group <y>
CLI(conf-voice-route)> exit
CLI(voice-route)> exit
```

6.2.4.2 Using FXS Voice Features

6.2.4.2.1 Call Waiting

An FXS subscriber has got one call in progress. When a second call destined to that subscriber comes in, the FXS subscriber hears a call waiting tone and the caller hears the phone ringing. The FXS subscriber may decide to put the active call on-hold (therefore the remote party placed on-hold hears the music-on-hold) and to accept the second call.

Call Waiting: Putting Active Call on-Hold and Accepting Second Call

Actions / Events on Phone	Comments
	One call is active.
"Beep"	The call waiting tone is played.
	Press hook flash button (R) followed by 2.
	You are connected with second caller.

6.2.4.2.2 Second Call

When a call is active, it is possible to put this call on hold, and then to call a second subscriber.

Making a Second Call

Actions / Events on Phone	Comments
	One call is active.
	Press hook flash button.
	A dialing tone is played. Dial the phone number of another subscriber.
	OneOS attempts to connect the call with the new subscriber.

6.2.4.2.3 Releasing Second Call

When a call is active and one on-hold, you can release the currently active call and switch to the other one.

Releasing Second Call

Actions / Events on Phone	Comments
	One call is active, one is on-hold.
	Press hook flash button followed by 1.
	You are now connected with the remote party that was on-hold. The remote that was previously active is now disconnected.

6.2.4.2.4 Brokering

Brokering is a feature related to an FXS subscriber having two SIP call legs. It refers to the action of switching between calls, i.e. putting one call on-hold and retrieving the other call (that was on-hold). The party on-hold hears the music-on-hold.

Brokering

Actions / Events on Phone	Comments
	Two calls are connected (one active, one on-hold).
	Press hook flash button followed by 2.
	You are now in communication with the party previously on-hold. The formerly active party is now on-hold.

6.2.4.2.5 Attended Call Transfer

Attended call transfer is also called call transfer with consultation.

A subscriber A is an FXS subscriber. Subscriber A is in conversation with subscriber B. Subscriber A puts subscriber B on hold. Subscriber A calls subscriber C. Subscriber A asks subscriber C if he wants to talk to subscriber B. Then, subscriber A initiates a call Transfer, so that subscriber B talks to subscriber C and the calls from subscriber A to subscriber B or subscriber C are released.

Attended Call Transfer

Actions / Events on Phone	Comments
	One call is active.
	Press hook flash button.
	A dialing tone is played. Dial the phone number of another subscriber.
	The new subscriber hangs up the phone.
	Hook-on, the call is transferred. *Note: depending of settings, the transfer can also be done with R4 instead of on-hook.*

6.2.4.2.6 Three-Way Conference

When an FXS subscriber has got two calls (one active, one on-hold) the FXS subscriber may decide to start a three-way conference. Three-way conference is started by pressing hook flash and 3.

Making a Second Call and Starting 3-Way Conference

Actions / Events on Phone	Comments
	One call is active.
	Press hook flash button.
	A dialing tone is played. Dial the phone number of another subscriber.
	OneOS attempts to connect the call with the new subscriber. The other subscriber's phone rings.
	The new subscriber answers.
	Press hook flash, then 3.
	3-way conference is started.

6.2.5 Obsolete Parameters

The following parameters are not used anymore but remain for configuration compatibility:

```
CLI(voice-port)> cas-conf

CLI(voice-port)> signal-analysis

CLI(voice-port)> metering

CLI(voice-port)> user-metering

CLI(voice-port)> without-loss-signal

CLI(voice-port)> coder-law
```

6.3 VOIP: ISDN INTERFACES CONFIGURATION

6.3.1 ISDN common parameters

This chapter describes the ISDN parameters that are common to the BRI and PRI interfaces. The ISDN parameters that are specific to these interfaces are described respectively in 6.3.2 "BRI Interface" and 6.3.3 "PRI Interface". All the following commands are entered in ISDN protocol configuration mode.

Enter the following command to specify the type of application that uses the interface; it must be set to `voip` if the interface is used by the SIP/H.323 gateway. Default: `voip`.

```
CLI(isdn)> application-interface { voip | voatm | data }
```

By default, the BRI/PRI interfaces use the Euro-ISDN protocol. In order to use EuroNumeris (France-specific, called also VN6), the next command has to be used:

```
CLI(isdn)> operator { euroisdn | euronumeris }
```

Enter the following command to specify the protocol emulation for layer 3 (network layer). Use `isdn-nt` for ISDN phone or for a PBX and `isdn-te` for connection to an ISDN network. Default: `isdn-te`.

```
CLI(isdn)> protocol-emulation { isdn-te | isdn-nt }
```

Use the following command to specify the protocol emulation for layer 2 (LAPD layer). Use it only if the layer 2 emulation must be different than the protocol emulation. Default: identical to protocol emulation.

```
CLI(isdn)> layer2-emulation { te | nt }
```

Use the following command to avoid the disconnection of the ISDN layer 2 when the ISDN terminal or the ISDN network disconnects the layer 2 (in static TEI mode); it will be maintained established. Default: `no`.

```
CLI(isdn)> [no] permanent-layer2
```

Use the following command to ignore the ISDN layer 2 N(S) field when receiving Information frames. Default: not ignored.

```
CLI(isdn)> no layer2-ns-check
```

Use the following command to remove the TEI also when the layer 2 is disconnected (in addition of the power-off condition):

```
CLI(isdn)> [no] tei-remove dl-connection-release
```

Use the following commands to specify the timer T301/T302/T303/T304/T305/T306/T308/T309/T310/T313 values for the network layer.

```
CLI(isdn)> t301-timer <10-2000: default 180 seconds>
CLI(isdn)> t302-timer <1-200: default 15 seconds>
CLI(isdn)> t303-timer <1-200: default 4 seconds>
CLI(isdn)> t304-timer <5-50: default 30 seconds>
CLI(isdn)> t305-timer <1-200: default 30 seconds>
```

```
CLI(isdn)> t306-timer <1-400: default 30 seconds>
CLI(isdn)> t308-timer <1-200: default 4 seconds>
CLI(isdn)> t309-timer <4-180: default 90 seconds>
CLI(isdn)> t310-timer <1-400: default 30 seconds>
CLI(isdn)> t313-timer <1-200: default 4 seconds>
```

Use the following command to specify the k parameter (window size) for the link layer. Default: 7.

```
CLI(isdn)> k-window <1..128>
```

Use the following command to specify the type of B-Channel sent to the TE. Default: exclusive (prior to V3.7R11E15 software release default value was preferred).

```
CLI(isdn)> b-channel { preferred | exclusive }
```

Use the following command to disable the transmission of FACILITY message. Some PBXs do not support this type of message. Default: enable.

```
CLI(isdn)> no facility
```

Use the following command to suppress any PROGRESS message sent to the ISDN device. Default: not suppressed.

```
CLI(isdn)> no progress
```

Use the following command to force the Progress-In-Band information element to be inserted in ALERTING message (which forces the B-channel to be connected) and the OneOS-based router to generate locally the ringback tone. This function must be used for PBXs that never generate a ringback tone and where the network does not provide a ringback tone either.

```
CLI(isdn)> [no] alert-ie-progress
```

Use the following command to suppress the signal information element for any ALERTING message sent to the ISDN device. Default: not suppressed.

```
CLI(isdn)> no alert-ie-signal
```

Use the following command to suppress the channel information element for any ALERTING message sent to the ISDN device. Default: not suppressed.

```
CLI(isdn)> no alert-ie-channel
```

Use the following command to suppress the progress information element for any message sent to the ISDN device. Default: not suppressed.

```
CLI(isdn)> no ie-progress
```

Use the following command to suppress the user to user information element for any message sent to the ISDN device. Default: not suppressed.

```
CLI(isdn)> no ie-uui
```

Use the following command to select the user to user service 1 option as specified in EN 300 286-1 when "local UUS negotiation" is selected. Default: implicit.

```
CLI(isdn)> uus1-mode { implicit | explicit }
```

Use the following command to select, when in NT mode, whether the channel information element is inserted in the first message only or in all messages. Default: first message only.

```
CLI(isdn)> ie-channel { first-message-only | all-message }
```

Use the following command to select which SIP information ("From" or "To" display-names) is mapped to the ISDN display information element for any message sent to the ISDN device. Default: calling-name.

```
CLI(isdn)> ie-display [called-name | calling-name]
```

Use the following command to suppress the display information element for any message sent to the ISDN device. Default: not suppressed (see above).

```
CLI(isdn)> no ie-display
```

Note: the two following commands are obsolete and replaced by the `ie-display` command:

Obsolete: Use the following command to define how to insert the calling name in the SETUP message: calling sub address, display IE or Keypad IE. Default: disabled (calling name is not inserted).

```
CLI(isdn)> [no] calling-name-ie { origin-sub-address | display| keypad }
```

Obsolete: Use the following command to define if the called name is inserted in the SETUP message or not. Default: inserted.

```
CLI(isdn)> [no] called-name-ie [dest-sub-address]
```

Use the following command to suppress the HLC information element for any message sent to the ISDN device. Default: not suppressed.

```
CLI(isdn)> no setup-ie-hlc
```

Use the following command to suppress the LLC information element for any message sent to the ISDN device. Default: not suppressed.

```
CLI(isdn)> no setup-ie-llc
```

Use the following command to insert the non-ISDN origination address progress description in the progress indicator information element if HLC / LLC not present. Default: not inserted.

```
CLI(isdn)> [no] insert-non-isdn-PI
```

Use the following command to define the Q.850 cause when the ISDN line is not operational. It is generally used to allow call forwarding. Default: 38 (network out of order).

```
CLI(isdn)> unavailability-q850cause <0-127>
```

If no channel is available to establish the call, the release cause is by default 34; the release cause can be changed as follows:

```
CLI(isdn)> channel-unavailable-cause { 17 | 34 }
```

Use the following command to choose the ISDN protocol monitoring option related to voice intrusive mechanism. Default: layer1

```
CLI(isdn)> intrusive-monitoring { layer1 | layer2 }
```

6.3.2 BRI Interface

If a BRI interface is used, it must be enabled by entering the following commands, which allows several parameters to be specified for the physical, link or network level.

Commands for enabling a BRI interface on physical port number n (voice module number 5):

```
CLI(configure)> interface bri 5/<n>
CLI(config-if)> [no] shutdown
CLI(config-if)>
```

The interface must be shut down if a parameter has to be modified. The interface is re-activated with the command `no shutdown`. When an interface is created, the default state is `shutdown`.

Enter the following command to enter the ISDN protocol configuration mode.

```
CLI(config-if)> isdn
CLI(isdn)>
```

Refer to 6.3.1 to configure most of the ISDN parameters that are common to all interfaces. The parameters specific to the BRI interface are described hereunder.

Enter the following command to specify the maximum number of simultaneous B channels. Default: 2

```
CLI(isdn)> max channels <0..2>
```

Use the following command to specify the protocol emulation for the physical layer. It must be configured only if the layer 1 emulation must be different than the protocol emulation. Default: identical to protocol emulation.

```
CLI(isdn)> layer1-emulation { te | nt }
```

Use the following command to maintain the ISDN layer 1 up; it is useful for clocking and management. Default: `no`.

```
CLI(isdn)> [no] permanent-layer1
```

Use the following command to avoid the disconnection of the ISDN layer 2 when there is no call in progress in dynamic TEI mode. Default: disconnection enabled.

```
CLI(isdn)> no lapd-disconnection-timeout
```

Use the following command to specify the TEI management mode. It must be set to `dynamic` for ISDN phones or connection to an ISDN network and `static` for PBX. Default: dynamic.

```
CLI(isdn)> tei-negotiation { dynamic | static }
```

Use the following command to define the TEI value in static mode. Default: 0.

```
CLI(isdn)> static-tei <0..63>
```

Use the following command to enable the lifeline bypass on the BRI S0 voice module. If the interface is used by the H.323/SIP gateway, the bypass is enabled if the OneOS-based voice-capable router is not registered with the gatekeeper (if configured). Use the `no` form to disable the lifeline bypass (default).

```
CLI(isdn)> [no] life-line-hold
```

Use the following command to specify the N200 parameter for the link layer.

```
CLI(isdn)> n200-counter <1-20:default 3>
```

Use the following command to specify the N202 parameter for the TEI management.

```
CLI(isdn)> n202-counter <1-20:default 2>
```

Use the following commands to specify the timer T200/T202/T203 values for the link layer.

```
CLI(isdn)> t200-timer <0-63: default 1 second>
CLI(isdn)> t202-timer <0-63: default 2 seconds>
CLI(isdn)> t203-timer <0-63: default 10 seconds>
```

Use the following command to specify modulo for NS/NR (link layer). Default: 128.

```
CLI(isdn)> modulo-window { 8 | 128 }
```

Use the following command to specify the type of channel for each B channel (1=B1, 2=B2). Several commands can be entered to specify several ranges of different types.

```
CLI(isdn)> ds0-group { incoming | outgoing | mixed | unused } { all
                                          | ts <1-2> | from <1-2> to <1-2> }
```

Type of channel:

- `incoming`: the channel is used only for calls coming from the ISDN device (PBX).
- `outgoing`: the channel is used only for calls being sent to the ISDN device.
- `mixed`: the channel can be used for incoming and outgoing calls (default value).
- `unused`: the channel cannot be used for calls.

Use the following commands to display the type of each B channel: I=Incoming; O=Outgoing; M=Mixed.

```
CLI(isdn)> display
CLI(display)> ds0-group
```

Note: the Channels #3 to #31 are not used (for PRI only).

Use the following command to allow two different methods for B channel allocation (regarding BRI/PRI interfaces) Default: first.

```
CLI(isdn)> ds0-alloc { older | first }
```

- `first`: allows B channel allocation from lowest available B channel (default value).
- `older`: allows B channel allocation from older available B channel (this method is useful when remote ISDN device needs a timeout to allow same B channel allocation).

Then, complete the ISDN configuration as follows:

```
CLI(isdn)> exit
CLI(config-if)> execute
CLI(config-if)> exit
CLI(configure)>
```

6.3.3 PRI Interface

If a PRI interface is used, it must be enabled by entering the following commands, which then allows several parameters to be specified for the physical, link or network level.

Commands for enabling an E1/T1 interface on physical port number 0 (voice module number 5):

```
CLI(configure)> interface pri 5/0
CLI(config-if)> [no] shutdown
CLI(config-if)>
```

The interface must be shut down if a parameter has to be modified. The interface is re-activated with the command `no shutdown`. When an interface is created, then default state is "shutdown".

Use the following command to specify the interface type of voice interface as E1 or T1 (default: E1).

```
CLI(config-if)> physical-interface { e1 | t1 }
```

Use the following command to specify the framing type.

```
CLI(config-if)> framing { none | df | mf | emf | sf | esf | auto-detect }
```

- `none`: no framing. Only used for CES / unstructured mode.
- `df`: double frame, no CRC4. For E1 only. (Default value).
- `mf`: multiframe (CRC4). For E1 only.
- `emf`: extended multiframe (CRC4). For E1 only.
- `sf`: super-frame (for T1 only).
- `esf`: extended super frame (for T1 only).
- `auto-detect`: used to find automatically ISDN PRI framing by trying all possible detections. This behavior can be set when the configuration of remote side is unknown. An event containing the correct framing is generated when layer-1 is activated.

Use the following command to specify the physical line coding to be used (default: hdb3).

```
CLI(config-if)> linecode { ami | hdb3 | b8zs }
```

Use the following command to enter in the protocol configuration.

```
CLI(config-if)> isdn
CLI(isdn)>
```

Refer to 6.3.1 to configure most of the ISDN parameters that are common to all interfaces. The parameters specific to the PRI interface are described hereunder.

Use the following command to specify the maximum number of simultaneous B channels. Default 30

```
CLI(isdn)> max channels <0..30>
```

Use the following command to specify the N200 parameter for the link layer.

```
CLI(isdn)> n200-counter <1-20:default 3>
```

Use the following commands to specify the timer T200/T203 values for the link layer.

```
CLI(isdn)> t200-timer <0-63: default 1 second>
CLI(isdn)> t203-timer <0-63: default 10 seconds>
```

Use the following command to specify the type of channel for each B channel (except #16, reserved for signaling). Several commands can be entered to specify several ranges of different types.

```
CLI(isdn)> ds0-group { incoming | outgoing | mixed | unused } { all
                                    | ts <1-31> | from <1-31> to <1-31> }
```

Type of channel:

- `incoming`: the channel is used only for calls coming from the ISDN device (PBX).
- `outgoing`: the channel is used only for calls being sent to the ISDN device.
- `mixed`: the channel can be used for incoming and outgoing calls (default value).
- `unused`: the channel cannot be used for calls.

Use the following commands to display the type of each B channel: I=Incoming; O=Outgoing; M=Mixed.

```
CLI(isdn)> display
CLI(display)> ds0-group

ts     1 – 2 – 3 – 4 – 5 – 6 -  7 -  8 -  9 – 10 – 11 – 12 – 13 – 14 – 15 – 16
type   M   M   M   I   I   I    I    I    M    M    M    M    M    M    M    x
ts    17 – 18 – 19 – 20 – 21 – 22 – 23 – 24 – 25 – 26 – 27 – 28 – 29 – 30 – 31
type   M    M    M    M    M    M    M    M    M    M    M    M    M    M    M
```

Use the following command to allow two different methods for B channel allocation (regarding BRI/PRI interfaces) Default: first.

```
CLI(isdn)> ds0-alloc { older | first }
```

- `first`: allows B channel allocation from lowest available B channel (default value).
- `older`: allows B channel allocation from older available B channel (this method is useful when remote Isdn equipment needs a timeout to allow same B channel allocation).

Then, complete the ISDN configuration as follows:

```
CLI(isdn)> exit
CLI(config-if)> execute
CLI(config-if)> exit
CLI(configure)>
```

6.4 VOIP: E1 R2 INTERFACE CONFIGURATION

6.4.1 CAS R2 profiles configuration

Prior to configure E1 R2 interface, profiles have to be defined. These CAS R2 profiles allow configuring the various parameters of the CAS R2 signaling.

To enter in CAS R2 profiles configuration, use the following commands in global configuration mode:

```
CLI(configure)> cas-r2
CLI(cas-r2)> profile <index:0..29>
CLI(cas-r2-profile)>
```

There are several flavor of E1 R2 signaling depending on countries. To define the flavor of E1 R2 signaling, use the following command in CAS R2 profile configuration mode:

```
CLI(cas-r2-profile)> country { ITU | Argentina | Brazil | China
                             | Czech-Republic | Colombia | Ecuador
                             | Mexico | Philippines | Venezuela }
```

Note that as of V4.2R7E2 software release, only profiles ITU (default value), Mexico and Philippines have been tested. Other profiles are available but not tested yet (contact OneAccess customer support department for more information).

As soon as the profile country is selected, the various parameters get their country-specific values (default values); these values can be listed using the `display` command described further in this section.

Note: from here the following commands in CAS R2 profile configuration mode are all optional; they can be used to specify another value than the default value. They must be used carefully by skilled people only when other values than default values are explicitly requested.

Default values given as example are the ones of the ITU profile.

To define the maximum number of digits for Automatic Number Identification (ANI=caller ID), use:

```
CLI(cas-r2-profile)> ani-digits <1..63:default 20>
```

To define the maximum number of digits for Dialed Number Identification Service (DNIS=called ID), use:

```
CLI(cas-r2-profile)> dnis-digits <1..63:default 20>
```

By default ANI digits are sent before DNIS digits, to reverse the order use:

```
CLI(cas-r2-profile)> no ani-first
```

To come back to the default behavior (ANI first), use:

```
CLI(cas-r2-profile)> ani-first
```

By default collect calls blocking is not enabled, to enable the feature (country specific) use:

```
CLI(cas-r2-profile)> double-answer <10..500 in ms>
```

To come back to the default behavior (no collect calls blocking), use:

```
CLI(cas-r2-profile)> no double-answer
```

By default voice traffic is immediately enabled after call acceptation, to disable the feature use:

```
CLI(cas-r2-profile)> no early-media
```

To come back to the default behavior (voice traffic immediately enabled), use:

```
CLI(cas-r2-profile)> early-media
```

By default calls are not accepted without the use of group B and II tones, to accept calls without group B and II tones use:

```
CLI(cas-r2-profile)> immediate-accept
```

To come back to the default behavior (use of group B and II tones is mandatory), use:

```
CLI(cas-r2-profile)> no immediate-accept
```

To set the maximum time (in seconds) the MF backward compelled signaling cycle may last, use:

```
CLI(cas-r2-profile)> mf-back-timeout <1..100:default 5s>
```

To set the maximum time (in seconds) the MF forward compelled signaling cycle may last, use:

```
CLI(cas-r2-profile)> mf-fwd-timeout <1..100:default 30s>
```

To set the minimum duration (in milliseconds) a MF signal must last to be detected, use:

```
CLI(cas-r2-profile)> mf-threshold <0..500:default 0ms>
```

To set the maximum time (in seconds) to wait for the seizing-acknowledgment signal, use:

```
CLI(cas-r2-profile)> seizure-ack-timeout <1..100:default 8s>
```

To set the maximum time (in seconds) to wait for the answer signal, use:

```
CLI(cas-r2-profile)> accept-answer-timeout <1..100:default 60s>
```

To set the minimum duration (in milliseconds) a CAS line signal must last to be taken into account, use:

```
CLI(cas-r2-profile)> cas-persistent-check <0..500:default 0ms>
```

CAS line signals use bits A and B of the associated channels; to set the value of unused bits C and D of the associated channels (default values C=0, D=1), use:

```
CLI(cas-r2-profile)> unused-bits c { 0 | 1 } d { 0 | 1 }
```

Use the following commands to define the multi-frequency combination for the group I forward signals:

```
CLI(cas-r2-profile)> g1 <signal>                  <MF-tone:0..15;0=none>
CLI(cas-r2-profile)> g1 no-more-dnis-available   <0..15:default 15>
CLI(cas-r2-profile)> g1 no-more-ani-available    <0..15:default 15>
CLI(cas-r2-profile)> g1 caller-ani-is-restricted <0..15:default 12>
```

Use the following commands to define the multi-frequency combination for the group II forward signals:

```
CLI(cas-r2-profile)> g2 <signal>                    <MF-tone:0..15;0=none>
CLI(cas-r2-profile)> g2 national-subscriber         <0..15:default 1>
CLI(cas-r2-profile)> g2 national-priority-subscriber <0..15:default 2>
CLI(cas-r2-profile)> g2 international-subscriber    <0..15:default 7>
CLI(cas-r2-profile)> g2 international-priority-subscriber <0..15:def.9>
CLI(cas-r2-profile)> g2 collect-call                <0..15:default 0>
```

Use the following commands to define the multi-frequency combination for the group A backward signals:

```
CLI(cas-r2-profile)> ga <signal>                <MF-tone:0..15;0=none>
CLI(cas-r2-profile)> ga request-next-dnis-digit <0..15:default 1>
```

```
CLI(cas-r2-profile)> ga request-dnis-1          <0..15:default 2>
CLI(cas-r2-profile)> ga request-dnis-2          <0..15:default 7>
CLI(cas-r2-profile)> ga request-dnis-3          <0..15:default 8>
CLI(cas-r2-profile)> ga request-all-dnis-again  <0..15:default 0>
CLI(cas-r2-profile)> ga request-next-ani-digit  <0..15:default 5>
CLI(cas-r2-profile)> ga request-category        <0..15:default 5>
CLI(cas-r2-profile)> ga request-categoty-and-change-to-gc <0..15:def.0>
CLI(cas-r2-profile)> ga request-change to g2    <0..15:default 3>
CLI(cas-r2-profile)> ga address-complete-charge-setup <0..15:default 6>
CLI(cas-r2-profile)> ga network-congestion      <0..15:default 4>
```

Use the following commands to define the multi-frequency combination for the group B backward signals:

```
CLI(cas-r2-profile)> gb <signal>                  <MF-tone:0..15;0=none>
CLI(cas-r2-profile)> gb accept-call-with-charge   <0..15:default 6>
CLI(cas-r2-profile)> gb accept-call-no-charge     <0..15:default 7>
CLI(cas-r2-profile)> gb busy-number               <0..15:default 3>
CLI(cas-r2-profile)> gb network-congestion        <0..15:default 4>
CLI(cas-r2-profile)> gb unallocated-number        <0..15:default 5>
CLI(cas-r2-profile)> gb line-out-of-order         <0..15:default 8>
CLI(cas-r2-profile)> gb special-info-tone         <0..15:default 2>
CLI(cas-r2-profile)> gb reject-collect-call       <0..15:default 0>
CLI(cas-r2-profile)> gb number-changed            <0..15:default 0>
```

Use the following commands to define the multi-frequency combination for the group C backward signals:

```
CLI(cas-r2-profile)> gc <signal>                  <MF-tone:0..15;0=none>
CLI(cas-r2-profile)> gc request-next-ani-digit    <0..15:default 0>
CLI(cas-r2-profile)> gc request-change-to-g2      <0..15:default 0>
CLI(cas-r2-profile)> gc request-next-dnis-digit-and-change-to-ga
                                                  <0..15:default 0>
```

Then, return in CAS R2 configuration mode to complete the CAS R2 profile configuration as follows:

```
CLI(cas-r2-profile)> exit
CLI(cas-r2)>
```

When in CAS R2 configuration mode, to display CAS R2 profile actual configuration, use:

```
CLI(cas-r2)> display [profile <index>]
```

Example:

```
CLI(cas-r2)> display profile 0
cas-r2
 profile 0
 exit
exit
CLI(cas-r2)>
```

Use the `complete` option to display the full actual configuration (including default values):

```
CLI(cas-r2)> display profile 0 complete
cas-r2
 profile 0
  country ITU
  ani-digits 20
  dnis-digits 20
  ani-first
  no double-answer
  early-media
  no immediate-accept
  mf-back-timeout 5
  mf-threshold 0
  seizure-ack-timeout 8
  accept-answer-timeout 60
```

```
  cas-persistence-check 0
  mf-fwd-timeout 30
  unused-bits c 0 d 1
  ga request-next-dnis-digit 1
  ga request-dnis-1 2
  ga request-dnis-2 7
  ga request-dnis-3 8
  ga request-all-dnis-again 0
  ga request-next-ani-digit 5
  ga request-category 5
  ga request-category-and-change-to-gc 0
  ga request-change-to-g2 3
  ga address-complete-charge-setup 6
  ga network-congestion 4
  gb accept-call-with-charge 6
  gb accept-call-no-charge 7
  gb busy-number 3
  gb network-congestion 4
  gb unallocated-number 5
  gb line-out-of-order 8
  gb special-info-tone 2
  gb reject-collect-call 0
  gb number-changed 0
  gc request-next-ani-digit 0
  gc request-change-to-g2 0
  gc request-next-dnis-digit-and-change-to-ga 0
  g1 no-more-dnis-available 15
  g1 no-more-ani-available 15
  g1 caller-ani-is-restricted 12
  g2 national-subscriber 1
  g2 national-priority-subscriber 2
  g2 international-subscriber 7
  g2 international-priority-subscriber 9
  g2 collect-call 0
 exit
exit
CLI(cas-r2)>
```

To remove a CAS R2 profile if needed, use the following command in CAS R2 configuration mode:

```
CLI(cas-r2)> no profile <index:0..29>
```

Then return in global configuration mode:

```
CLI(cas-r2)> exit
CLI(configure)>
```

6.4.2 E1 R2 interface configuration

The configuration of the E1 R2 interface is achieved in interface PRI configuration mode.

- The interface PRI must be in shutdown state to take into account the configuration commands.
- The changes are applied only when the no shutdown command is entered (error and warning messages, if any, are displayed at that time).
- The CAS R2 section deletes the ISDN section if there is one in interface PRI configuration.

```
CLI(configure)> interface pri 5/0
CLI(config-if)> shutdown
CLI(config-if)> cas-r2
Warning: group 1 ts 1-15,17-31 profile 0 created
Warning voice-port 5/0.1 created
CLI(cas-r2)> exit
CLI(config-if)> no shutdown
CLI(config-if)> exit
```

```
CLI(configure)>
```

When `cas-r2` command is entered the first time,

- The CAS group 1 is automatically created with all available time slots and CAS R2 profile 0 is applied.
- Voice port 5/0 is deleted and replaced by `voice-port 5/0.1` (one sub voice port per CAS group).

To modify the time slots allocation in CAS groups, apply a CAS R2 profile and optionally define the mode of allocation use the `group` command in CAS R2 configuration mode:

```
CLI(configure)> interface pri 5/0
CLI(config-if)> shutdown
CLI(config-if)> cas-r2
CLI(cas-r2)> group <1..10> ts <list> profile <index> [mode {first|last}]
CLI(cas-r2)> exit
CLI(config-if)> no shutdown
CLI(config-if)> exit
CLI(configure)>
```

`list` is the list of the time slots that are placed in the group. Example: `ts 1-15,17,24-31`.

`index` is the number of the CAS R2 profile that is used for the CAS R2 signaling of the group.

`mode` defines how time slots are allocated for outbound calls; the `first` (default) or the `last` available.

- Time slots 0 and 16 cannot be used.
- Unused time slots are put in blocked state (time slots 18 to 23 in the example above).
- Sub voice ports are created as soon as the groups are created (one sub voice port per group).
- When a sub voice port is put in shutdown mode all corresponding time slots are put in blocked state.

A command is added in (sub) voice port configuration to allow the OneOS-based voice-capable router adding the local ringback tone when no ringback tone is received on the R2 port. The following command must NOT be entered as default because the R2 ringback signal would be added to the local ringback.

```
CLI(voice-port)> [no] r2-reverse-ringback-tone
```

Then the R2 sub voice port can be used as regular voice port in a dial peer voice POTS for VoIP configuration (see next chapter). For example:

```
configure terminal
  dial-peer voice pots 0
    pots-group 1
    port 5/0.1
    no shutdown
    exit
```

6.5 VOIP: INTERNAL LOCAL VOICE PORT CONFIGURATION

The command for the creation of a local voice port associated with the 5/p physical port is:

```
CLI(configure)> dial-peer voice pots <n>
CLI(pots)> port 5/<p>
```

Each dial-peer voice POTS (analog or ISDN) must be identified by an arbitrary index n from 0 to N. The physical port numbering is defined in the product installation manual.

Use the following command to indicate the group the port belongs to. In a group all the ports have the same phone number. Default: the port belongs to pots-group 0 with priority defined in `priority` command.

```
CLI(pots)> [no] pots-group <0..30> [priority <0..30>]
```

Use the following command to optionally indicate the voice group the port belongs to. A voice group can contain POTS and VoIP ports.

```
CLI(pots)> [no] voice-group <0..30> [priority <0..30>]
```

Use the following command to define the default priority of the port in the group (if not defined in the `pots-group` or `voice-group` command). In the group all the interfaces with the same priority are selected circularly (round robin) or according to the load (load balancing). Default: 0.

```
CLI(pots)> [no] priority <0..30>
```

Use the following command to enable the suppression of n digits at the beginning of the calling number for calls coming from the device attached to the port.

```
CLI(pots)> [no] suppress-calling-number <1-35>
```

Use the following command to insert a number at the beginning of the calling number for calls coming from the device attached to the port. If `suppress-calling-number` is enabled, the specified `number` replaces the beginning of the calling number. `number` is made of 1 to 35 (0-9, #, *****) characters.

On FXS interfaces with SIP, this argument is mandatory; otherwise the calling number in the "From" and "Contact" fields will be empty.

```
CLI(pots)> [no] insert-calling-number <number>
```

Use the following command to enable a direct call to the specified number when detecting an off-hook (for analog ports only). The `number` is made of 1 to 35 (0-9, #, *****) characters.

```
CLI(pots)> [no] direct-call <number>
```

Use the following command to enable implicit routing. All the incoming calls are routed to the specified port or group of ports without any analysis of the destination number.

```
CLI(pots)> [no] implicit-routing { pots | pots-group | voip | voip-group
                                 | voice-group } <port-identifier: 0-30>
```

Use the following command to specify the emergency level for any call arriving on this port. Default: 100.

```
CLI(pots)> [no] emergency <1..200>
```

Use the following command to define the bearer capability to be used for inbound call coming from FXS ports only. Default: voice.

```
CLI(pots)> bearer-cap { voice | voice-band | unrestricted }
```

Use the following command to make CLIP encoding being in conformance with Q.951 clause 3. When CLIP is in force and no calling number is present in ISDN SETUP message, the presentation indicator is forced to "Number not available due to interworking" (2) and the screening indicator is forced to "Network provided" (3). When calling number is present, the presentation indicator is forced to "Presentation restricted" (1) and the screening indicator is forced to "Network provided" (3) when `modified` is used or they remain unchanged when `transparent` is used.

```
CLI(pots)> [no] q951-conformance { transparent | modified }
```

Use the following command to define the maximum number of simultaneous voice calls.

```
CLI(pots)> [no] max-conn <0..32>
```

This parameter depends on interface type:

ISDN PRI: 32 calls (300 calls on ONE300)	[default: 32]
ISDN BRI: 4 calls (2 with B-channel + 2 without channel)	[default: 4]
FXS: 3 calls with intelligent profile and IBC	[default: 3]
FXS: 2 calls with intelligent profile and not IBC	[default: 2]
FXS: 1 call without intelligent profile	[default: 1]
FXO: 1 call	[default: 1]

Use the following command to define the Q.850 cause value when `max-conn` is exceeded (default 47).

```
CLI(pots)> max-conn-q850cause <cause>
```

The following commands are used for the routing process. They are described in the corresponding chapter (see 7.2).

```
CLI(pots)> default-type-of-number

CLI(pots)> numplan-preprocessing

CLI(pots)> dial-plan

CLI(pots)> international-numplan

CLI(pots)> national-numplan
```

6.6 VOIP: H.323 GATEWAY CONFIGURATION

The following command enters the global parameters configuration for the H.323 gateway:

```
CLI(configure)> h323-gateway
CLI(h323gw)>
```

Use the following command to shutdown the H.323 gateway. Changes on some parameters concerning the H.323 gateway require a shutdown/no shutdown operation. After a "shutdown", the gateway sends a deregistration request. Default: shutdown.

```
CLI(h323gw)> [no] shutdown
```

Use the following command to define the IP interface attached to the H.323 gateway (may be Ethernet, FastEthernet, ATM, PPP…). The IP address of the H.323 gateway (for registering to a gatekeeper, for example) is the IP address configured for this interface (if the `gw-address` command parameter is configured `implicit`).

If the `intrusive` option is enabled, the H.323 gateway is started when the IP interface goes up and is deactivated if the IP interface becomes down (all the current calls are cleared). If the `monitoring` option is also enabled, the H.323 gateway is started when the dialer watch-list goes up and is deactivated if the dialer watch list becomes down (all the current calls are cleared). The dialer watch-list monitoring is more precise than the simple interface monitoring.

```
CLI(h323gw)> [no] gw-interface <source-interface> <unit>
                  [intrusive [monitoring dialer-watch-list <list-name>]]
```

Use the following command to specify if the IP address of the H.323 gateway is the one of the interface defined by the `gw-interface` command or another one acquired by the autoconfiguration process (see "Autoconfiguration" chapter of "OneOS – Admin User Guide" document). Default: implicit.

```
CLI(h323gw)> gw-address {implicit | autoconfig}
```

Use the following command to configure the gatekeeper identifier and IP address. Both parameters are optional: if the IP address is not configured, the automatic discovery is enabled. To work without a gatekeeper, `no gatekeeper` must be entered (default value).

```
CLI(h323gw)> [no] gatekeeper [id <gatekeeper-identifier>]
                             [ipaddr <IP-address>:<RAS port>]
```

Use the following command to set the alternate gatekeeper mode. If dynamic, the OneOS-based voice-capable router takes into account the list of alternate gatekeeper given by the gatekeeper in the RAS protocol. If static the configured list is used. Default: static.

```
CLI(h323gw)> altgk-mode { static | dynamic }
```

Use the following command to specify a timer for checking the primary gatekeeper when the device is registered with an alternate gatekeeper. Use the `no` form to disable the periodic checking (default).

```
CLI(h323gw)> [no] altgk-timeout <seconds>
```

Use the following command to enter in the alternate gatekeeper list configuration.

```
CLI(h323gw)> altgk-list
```

```
CLI(h323gw-altgk)>
```

Then, use the following command to configure an alternate gatekeeper with a priority (default: 127), an identifier, an IP address, and “needed” if the registration must be maintained. Use the `no` form with `index` to suppress a gatekeeper. The enter `exit` to return to the H.323 gateway configuration mode.

```
CLI(h323gw-altgk)> [no] altgk <index 1-5> [priority <1-127>] id
<gk-identifier> address <IP-addr>:<RAS-port> [register { needed | no }]
…...
CLI(h323gw-altgk)> exit
```

Use the following command to configure a backup gatekeeper (same parameters as above). This command equivalent to the `altgk-list` above is deprecated and remains for compatibility.

```
CLI(h323gw)> alt-gatekeeper id <gatekeeper-identifier>
                            ipaddr <IP-address>:<RAS-port>
```

Use the following command to enable the Resource Management using the RAS RAI procedure. The criteria may be the B Channel allocation ratio or the bandwidth (defined in 5.2.2) ratio or both. Two thresholds are defined: a low water mark and a high water mark (in percentage).

```
CLI(h323gw)> [no] resource threshold { all | ds0 | bandwidth }
                                                high <0-100> low <0-100>
```

Use the following command to link H.323 gateway and voice port status.

```
CLI(h323gw)> [no] ras-intrusive-voiceport { registration-status
                  | both-way} { and-mode | or-mode } <5/0,5/2… ,voip/0,…>
```

- Impact of the port status on the registration: `and-mode` means that all the specified ports must be up for starting the registration; `or-mode` means that the registration process will start if one or more of the ports are up.
- `both-way` forces a bi-directional intrusive mode. If H.323 is not registered, the list of ports is set down and if the list of ports is not up, the H.323 gateway is de-registered.
- Impact of the registration status on the voice port status: `registration-status` means that the specified ports are deactivated when the H.323 gateway is not registered.
- The list of ports includes ISDN voice ports (5/0, 5/1 …) or VoIP trunks to an IP-PBX (`voip-group 0`, `voip-group 1` …).

Use the following command to force the state of the number portability function. The timeout parameter is optional and specifies the duration of the "in-progress" state. The default value is 5760 minutes (4 days). Use the `no` form to disable the portability function (default).

```
CLI(h323gw)> set-portability { enable | in-progress | done }
                                      [timeout <time-in-minutes 1-525600>]
```

Use the following command to define the H.323 identifier for the gateway (optional). The identifier is a 1 to 40 characters length string.

```
CLI(h323gw)> h323-id <string>
```

Use the following command to define the email identifier for the gateway (optional). The identifier is a 1 to 40 characters length string.

```
CLI(h323gw)> email-id <string>
```

Use the following command to define the gateway prefix indicated in the registration message. The number is made of 1 to 35 (0-9, #, *****) characters.

```
CLI(h323gw)> gw-prefix <number>
```

Use the following command to define the IP multicast address and port for gatekeeper discovery (default: 204.2.3.41:1718).

```
CLI(h323gw)> ras-multicast <IP-address>:<port>
```

Use the following command to define the UDP port used for RAS protocol (default: 1719).

```
CLI(h323gw)> ras-port <0-65535>
```

Use the following command to define the H.225/Q.931 listening TCP port (default: 1720).

```
CLI(h323gw)> callsig-port <0-65535>
```

Use the following command to enable (disable) the TCP keepalive procedure for H.323 sessions. Default: enable.

```
CLI(h323gw)> [no] tcp-keepalive
```

Use the following command to define the UDP port range used for RTP (each 0-65535). Default 16384-16482.

```
CLI(h323gw)> rtp-port-range min <0-65535> max <0-65535>
```

Use the following command to force the use of the same ports RTP and RTCP in case of new codec or T38 negotiation during the communication.

```
CLI(h323gw)> [no] fixed-media-port
```

Use the following command to define the RTP payload type value (ex: 101) for Unrestricted Data flows (UDI 64K). Default: G.711 (Clearmode) value i.e. 125.

```
CLI(h323gw)> payload-64k-unrestricted <0-255>
```

Use the following command to define the timeout for the response to a SETUP message Default: 10 sec.

```
CLI(h323gw)> q931-response-timeout <1-300>
```

Use the following command to define the timeout for receiving CONNECT message. Default: 10 sec.

```
CLI(h323gw)> q931-connection-timeout <1-300>
```

Use the following command to define the timeout used for RAS protocol. Default: 10 sec.

```
CLI(h323gw)> ras-response-timeout <1-300>
```

Use the following command to define the retries number in case of no response coming from the gatekeeper before trying the alternate gatekeeper. Default: 3.

```
CLI(h323gw)> ras-max-retries <1..200>
```

Use the following command to define the time-to-live value indicated in the Registration Request. Default: 60 sec.

```
CLI(h323gw)> ras-timetolive <1..300>
```

Use the following command to define the timeout value for light registration retries. It must be lower than the time to live. Default: 45 sec.

```
CLI(h323gw)> ras-keepalive-timeout <1..200>
```

If H.235 is used and the server does not require full registration, light re-registration is sent by the OneOS-based device. Use the following command to force full RAS registration periodically after the timeout defined in the command. Use the no form to use light re-registration (default).

```
CLI(h323gw)> [no] ras-full-reg-timeout <timeout>
```

Use the following command to define the timeout used for H.245 protocol. Default: 10 sec.

```
CLI(h323gw)> h245-response-timeout <1-300>
```

Use the following command to enable the transmission of RAS Bandwidth Requests messages toward the Gatekeeper for bandwidth control. Default: disabled.

```
CLI(h323gw)> [no] ras-bandwidth-control
```

Use the following commands to force the registration and the unregistration. Unregistration must be done before a reboot to keep a correct registration state in the gatekeeper.

```
CLI(h323gw)> register
CLI(h323gw)> unregister
```

Use the following command to discard the facility start h245 sent by the remote.

```
CLI(h323gw)> [no] start-h245-discarded
```

Use the following command to enable the H.235 authentication procedure for RAS. The optional parameter type allows hiding the password in the CLI text file and for a show running-config command. The type ‘0’ indicates that the password must be encrypted. The type ‘1’ indicates that the password is encrypted. If type is absent, the password is not encrypted. If the password is entered in clear mode with type=0, it will appear encrypted with type set to 1 in the configuration file. Default: h235 disable.

```
CLI(h323gw)> [no] h235-authentication <username> <password> [<type>]
```

Use the following command to perform three test calls after successful H.323 gateway registration. The H.323 call is placed through the gatekeeper using the calling and called phone number provided as command arguments. If, at least, one of the three successive calls is successful (as far as signaling for call establishment is concerned), the voice gateway of the router is considered operational and the LED marked "Voice" is green. Otherwise, the LED is red, until a successful voice call goes through (call initiated by a local subscriber).

```
CLI(h323gw)> call-test called <e164-number> calling <e164-number>
```

Use the following command to enable a specific format for the SNMP sysdescr object with a description of the voice hardware configuration. Default: disabled.

```
CLI(h323gw)> [no] snmp-sysdescr-hw-ident
```

Use the following command to enable (disable) the TCP keepalive procedure for H.323 sessions. Default: enable.

```
CLI(h323gw)> [no] tcp-keepalive
```

Some firewalls / SBC may not allow re-negotiating another RTP port when a call is established. When the 'fixed-media-port' option is set, the same RTP port is used even if the codec is re-negotiated or if the communication switches to T.38. (Default: `no fixed-media-port`).

```
CLI(h323gw)> [no] fixed-media-port
```

Use the following command for a debug purpose only. It must not be used in normal conditions.

```
CLI(h323gw)> polling
```

Example:

```
h323-gateway
  gw-interface ATM 0.1
  gatekeeper id ZONE1 ipaddr 10.2.2.1:1718
  alt-gatekeeper id ZONE1 ipaddr 10.3.2.1:1718
  h323-id GW1
  gw-prefix 20#
  ras-multicast 204.2.3.41:1718
  ras-port 1719
  callsig-port 1720
  rtp-port-range 32000 36000
  rtp-dscp 63
  q931-response-timeout 10
  q931-connection-timeout 10
  ras-response-timeout 10
  h245-response-timeout 10
  no shutdown
```

6.7 VOIP: SIP GATEWAY CONFIGURATION

The following command enters the parameters configuration for the SIP gateway:

```
CLI(configure)> sip-gateway
CLI(sipgw)>
```

Use the following command to shutdown the SIP gateway. Changes on some parameters concerning the SIP gateway require a shutdown/no shutdown operation. After a "shutdown", the gateway sends a deregistration request. Default: shutdown.

```
CLI(sipgw)> [no] shutdown
```

6.7.1 Parameters for Signaling

Use the following command to define the IP interface attached to the SIP gateway (may be Ethernet, FastEthernet, ATM, PPP ...). The IP address of the SIP gateway (for registration for example) is the IP address configured for this interface.

If the `intrusive` option is enabled, the SIP gateway is started when the IP interface goes up and is deactivated if the IP interface becomes down (all the current calls are cleared). If the `monitoring` option is also enabled, the SIP gateway is started when the dialer watch-list goes up and is deactivated if the dialer watch list becomes down (all the current calls are cleared). The dialer watch-list monitoring is more precise than the simple interface monitoring.

```
CLI(sipgw)> [no] gw-interface <source-interface> <unit> [intrusive
                              [monitoring dialer-watch-list <list-name>]]
```

Use the following command to define the UDP listening port for SIP. Default: 5060.

```
CLI(sipgw)> callsig-port <port>
```

Use the following command to define the DSCP field value for transmitted SIP packets. Default: 0.

```
CLI(sipgw)> sig-dscp <0-63>
```

6.7.2 Parameters for Registration

Use the following command to define an optional outbound-proxy. If enabled, all the SIP messages (signaling and registration) are sent to the specified IP address. If not used, the messages are sent to the configured SIP proxy and registrar. Default: not used.

```
CLI(sipgw)> [no] outbound-proxy <IP-address or domain-name>
```

Use the following command to define the registrar IP address or name (default port 5060). The "via" optional parameter defines an outbound proxy (all the registration messages will be sent to this address).

```
CLI(sipgw)> [no] reg-dns-add { <ip-address>[:<port>] | <dns-name> }
                                                    [via <ip-address>]
```

Use the following command to define the behavior of the SIP gateway when DNS resolution is used.

```
CLI(sipgw)> dns-resolution { current | first | first-only }
```

`first`: the request message is successively sent to all IP addresses given by the DNS response starting always with the first IP address until a response occurs.

`Current`: the request message is successively sent to all IP addresses given by the DNS response starting with the current IP address until a response occurs. In this mode, current IP address should normally be the available one.

`First-only`: the request message is always sent to the first IP address given by the DNS response. Others IP addresses are ignored.

Use the following command to configure the time interval between keepalive to check access to the registrar. `Interval` is provided in second granularity. Default: 1800 seconds).

```
CLI(sipgw)> reg-ka <interval>
```

The default mode is to re-register according to the "expires" value (or the `reg-ka` value if "expires" is not used). Use the following command to specify a custom behavior of the re-registration process.

```
CLI(sipgw)> [no] reg-ka-mode { percent | fixed | minus } <value-less>
              [limit <value> { percent | fixed | minus } <value-more>]
```

If `limit` is not specified the timer interval is calculated from the "expires" value (`value-less`% of "expires" or fixed `value-less` value or "expires" minus `value-less`).

If `limit` is specified, the timer interval is calculated depending on the relative values of `limit` and "expires".

- If "expires" is lower than or equal to `limit` the timer interval is calculated from the "expires" value (`value-less`% of "expires" or fixed `value-less` value or "expires" minus `value-less`).
- If "expires" is strictly greater than `limit` the timer interval is calculated from the "expires" value (`value-more`% of "expires" or fixed `value-more` value or "expires" minus `value-more`).

Example: `reg-ka-mode percent 50 limit 1200 minus 600` means that the re-registration timer is 50% of "expires" if "expires" is less than 1200 or "expires" minus 600 if "expires" is more than 1200.

Use the following command to select a specific external SIP proxy to be used when initiating a SIP outgoing call. `Via` optional parameter defines an outbound proxy (all the SIP signaling messages will be sent to this address).

```
CLI(sipgw)> [no] prox-dns-add { <proxy-ip-address>[:<port>]
                              | <proxy-name>[:<port>] }
                              [via <ip-address>[:<port>]]
```

Use the following command to configure the gateway SIP identifier for registration. `Username` is a string of up to 120 characters long. Note: the command `sip-id` is deprecated.

```
CLI(sipgw)> [no] sip-username <username>
```

Use the following command to configure the default SIP username and password for authentication. It is used if there is no sip-authentication command in the routing rules. `Sip-authentication` can be used for registration and invite authentication. The optional parameter `type` allows hiding the password in the CLI text file and for a `show running-config` command. `Type=0` indicates that the password must be encrypted. `Type=1` indicates that the password is already encrypted. If the parameter `type` is absent then the password is unchanged (not encrypted).

```
CLI(sipgw)> [no] sip-authentication <username: 1-120 char>
                                    [<password: 1-100 char>] [<type>]
```

Use the following command to define the hostname than can be used instead of an IP address in REGISTER and INVITE (see `uri-contact` and `uri-from` commands). `Host-name` is a string of up to 35 characters long. Use the `no` form to remove the hostname. Note: the command `sip-host-name` is deprecated.

```
CLI(sipgw)> [no] device-host-name <host-name>
```

The following parameter is obsolete and not used anymore but remains for configuration compatibility:

```
CLI(sipgw)> prox-ka
```

6.7.3 Tuning of SIP Messages

Use the following command to enable the SIP trunking mode. For outbound INVITE message, a P-Preferred-Identity header is added with the name indicated by sip-username and there is only one Registration session for the trunk (the routing table is not checked for multiple registrations). Default: disable.

```
CLI(sipgw)> [no] trunking-mode
```

Use the following command to specify if the hostname (if configured) or the IP address must be used in the “From” header field. Default: hostname if configured otherwise the IP address of the interface attached to the SIP gateway will be used.

```
CLI(sipgw)> uri-from { ip-address | hostname }
```

Use the following command to specify the “Contact” header field. By default, for the "host" part, the hostname, if configured, will be used; otherwise the IP address of the interface attached to the SIP gateway will be used. `String` (a 35-char string [0-9,*,#] at most) is used as the "user" part of the “Contact” header field. By default if contact-string is not defined, the "user" part of the “From” header field will be used.

```
CLI(sipgw)> uri-contact {ip-address | hostname} [contact-string <string>]
```

Use the following command to allow to send the BYE message when REFER is received. This behavior is required by some SIP proxies. Default: disable.

```
CLI(sipgw)> [no] bye-on-refer
```

Use the following command to allow to send the BYE message when a 202 OK is received (after having sent a REFER). Default: enable.

```
CLI(sipgw)> [no] bye-on-refer-accept
```

Use the following command to customize OneOS behavior for certain softswitch. When choosing `broadworks`, their proprietary management of call-waiting tone and hookflash is activated.

```
CLI(sipgw)> softswitch-profile { default | broadworks }
```

As of V3.7R10, the command `softswitch-profile` is deprecated and overridden by the command below.

Use the following command to enable a `Broadworks` specific mode to transport the hookflash event in SIP. Default: disable

```
CLI(sipgw)> [no] privacy-hookflash
```

Use the following command to include the field user agent in SIP headers; this can be useful for certain softswitch to apply varying processing based on the product manufacturer or hostname. If included, the default is to include the manufacturer information in user-agent field. Default: exclude.

```
CLI(sipgw)> user-agent {include [hostname | manufacturer] | exclude}
```

Use the following command to make any call aimed to be routed towards SIP Gateway interface to be checked. It must have its calling number registered and, as a consequence, must be known by the SIP Registrar/proxy at the remote endpoint of the current SIP Gateway interface. By default the checking is active.

```
CLI(sipgw)> [no] calling-number-checking
```

By default, the ***** and # digits are sent as is in URI. For compliance with the standards, use the following command to transform ***** and # with escape characters (i.e. %<ascii-code>).

```
CLI(sipgw)> [no] sip-uri-escape
```

A 3xx response code to an INVITE means that the sip-gateway should attempt another INVITE to a moved location. By default, the response code "302 Moved" is supported. Use the following command to clear the call upon receiving 3xx response.

```
CLI(sipgw)> [no] discard-3xx
```

Use the following command (with incoming or both-way) to define a specific URI (case-insensitive) that when received in the "From" header field of any incoming INVITE acts for the CLIR service. The default (standard) value is "anonymous@anonymous.invalid" for incoming calls.

Use the following command (with outgoing or both-way) to define the specific URI that will translate the CLIR service in the "From" header field of any outgoing call. This feature can be used if the softswitch does not support "Privacy" header, which is the recommended way to provide CLIR service. Default: disable. This command (with outgoing) obsoletes the `presentation-restricted` command.

```
CLI(sipgw)> [no] clip-privacy-uri <uri> [incoming | outgoing | both-way]
```

Use the following command to define the URI that, if contained in the "From" header field, makes the CLIP service to be not offered. The value depends on the SIP provider (not standardized). Default value: empty.

```
CLI(sipgw)> [no] clip-unsubscribe-uri <uri>
```

Use the following command to define how the called number of an inbound SIP call is extracted prior to be taken into account by voice routing to route the call. The default behavior is to look for a well-formatted phone number in examining the following header fields: "Request URI" then "P-Called-Party-ID" and "To".

Use `uri`, `p-called-party-id` and `to` strings separated by commas to define the order in which the headers are examined. Example for the default behavior: "`uri,p-called-party-id,to`".

```
CLI(sipgw)> sip-called-number <comma-separated-ordered-header-list>
```

Use the following command to force in SIP request message the display-name string contained in "From" header field.

```
CLI(sipgw)> [no] sip-from-display <string-up-to-50-char>
```

Use the following command to insert the calling information into P-Asserted-Identity field in SIP request message. This option is used for the CLIP service when the network is not able to check and assert the calling number.

```
CLI(sipgw)> [no] sip-asserted-id
```

Use the following command to insert the calling information also into P-Preferred-Identity field in SIP request message if needed.

```
CLI(sipgw)> [no] sip-preferred-id
```

Use the following command to define the request URI for the Conferencing Bridge. See 6.2.4.1 for more details.

```
CLI(sipgw)> [no] bridge-uri-host <hostname-or-ip>
```

The following command is deprecated.

```
CLI(sipgw)> [no] message-waiting-indication
```

6.7.4 SIP Timers

Use the following command to define in seconds the time-out to get a final response to an INVITE. If the timeout is 0, the "Expire" field of the INVITE request is removed. The main interest of reducing this timer is to detect earlier that an INVITE fails; then, voice-routing can re-route the call to a backup destination.

```
CLI(sipgw)> invite-method-timeout <seconds>
```

Use the following command to define in seconds the request time-out for a SIP message sent without a remote answer. The message is resent with a time interval that is doubled at every retransmission (first timeout is 500 ms) and so repetition is executed until the global timeout is expired. The command is applicable to any SIP request and especially for INVITE. By default, the timer is 32 sec. Use the no form to restore the default timer. The main interest of reducing this timer is to detect earlier that an INVITE fails; then, voice-routing can re-route the call to a backup destination.

```
CLI(sipgw)> [no] request-primitive-timer <seconds>
```

Use the following command to define in hours the maximum duration of a SIP communication. Default value is 0 (timer is disabled); recommended value is 18 hours. Use the no form to disable the bye timer.

```
CLI(sipgw)> [no] bye-timer <duration 0-24h>
```

Use the following command to define, for an outgoing call, the maximum time between reception of 1xx message (except 100 trying) and 200 OK. Default value is 0 (timer is disabled); recommended value is 180 sec. Use the no form to disable the connect timer.

```
CLI(sipgw)> [no] connect-timer <duration 60-300s>
```

Use the following command to define, for an outgoing call, the maximum time between the transmission of INVITE and the reception of 1xx message (except 100 trying) or 200 OK. Default value is 0 (timer is disabled); recommended value is 32°sec. Use the no form to disable the invite response timer.

```
CLI(sipgw)> [no] invite-response-timer <duration 10-50s>
```

Use the following command to define the timer used to send again a registration request, in case of reception of 4xx, 5xx, 6xx message. Default: 4 sec.

```
CLI(sipgw)> reg-failure-timer <duration 1-50s>
```

Use the following command to define the duration between two registration request sequences (`max-retry-nb` successive registration requests within the period defined buy request-primitive-timeout). Default: 1 sec and 0 retry.

```
CLI(sipgw)> reg-interval-timeout <duration 1-43200s> max-retry-nb <0-30>
```

Use the following command to define the timer used to go to the unregistered state in case of no reply of registration requests sent for keep-alive. Default: 3 sec.

```
CLI(sipgw)> [no] registration-timeout <duration 1-30s>
```

6.7.5 RTP Parameters

Use the following command to define UDP port range used for RTP (each 0-65535). Default 16384-16482.

```
CLI(sipgw)> rtp-port-range <0-65535> <0-65535>
```

By default, ISDN calls with unrestricted bearer capability are transported via a G.711 codec over IP (Clearmode). Use the following command to override the default RTP payload type and packet-time values for unrestricted data flows (UDI 64K). The command was created as a workaround for interoperability with non-standard compliant gateways. The default values are 125 (payload type) and 20 ms (packet-time).

```
CLI(sipgw)> [no] payload-64k-unrestricted <96-127> [10|20]
```

Warning: because of bandwidth control, when the local packet-time must be set to 10 ms (increased bitrate), the call may failed. In order to avoid this case, the following command must be added under sip-gateway (see 10.2).

```
CLI(sipgw)> bandwidth-control ratio 100 rate current-rate
```

Use the following command to define the DSCP field value for transmitted RTP packets (0-63). Default: 0.

```
CLI(sipgw)> rtp-dscp <0-63>
```

6.7.6 Intrusive voice port mode

Use the following command to make the status of the voice ports follow the status of the SIP gateway. It is used when the SIP gateway is considered as down to set down the designated voice ports. For example: to inform alarm device on FXS port (with the FXS power drop) that calls are no more possible or ISDN PBX to backup the calls on other ISDN lines or SIP PBX that calls are no more possible.

```
CLI(sipgw)> [no] intrusive-voiceport { atm-if-status
| sip-gateway-if-status | registration-status | registration-error
| port-registration-error | sip-monitoring | sip-monitoring-all }
[<5/u,5/v,5/w,voip/x,voip/y,voip/z>]
```

- `<5/u,5/v,5/w,voip/x,voip/y,voip/z>`: is the list of voice ports (separated by commas) which are handled. It includes FXS, BRI and PRI voice ports (`5/0`, `5/1` …) as well as VoIP trunks to an IP-PBX (`voip/0`, `voip/1` …). The list can be empty; in that case all existing ports are handled.

The following (exclusive) conditions can be tested for the status of the SIP gateway:

- `atm-if-status`: the SIP gateway is considered as down when the ATM line is down. This option may be used if the SIP gateway is not attached to an ATM interface but if the SIP traffic goes through the ATM link.
- `sip-gateway-if-status`: the SIP gateway is considered as down when the IP interface to which the gateway is attached is down.
- `registration-status`: the SIP gateway is considered as down when all phones (with `ua-sip` attribute including, if configured, the SIP gateway global registering) are not registered.
- `registration-error`: the SIP gateway is considered as down when one of the phones (with `ua-sip` attribute) is not registered.

Use the following condition to apply the power drop only to the designated port because of one or all of the above conditions are met:

- `port-registration-error`: only the designated ports are affected (downed) when the SIP gateway is considered as down (because the ATM line is down or the IP interface is down or the gateway is not globally registered) or the designated ports are not registered. Example: power drop is applied to port 5/0 if registration of port 5/0 is in error.

It is possible to take into account the SIP statuses of the dial-peer VoIP linked to the SIP gateway (see sip-monitoring command under dial-peer VoIP configuration) instead of the SIP gateway status (for example in case of registration process is not used):

- `sip-monitoring`: the SIP gateway is considered as down when one of the dial-peer VoIP linked to the SIP gateway is down.
- `sip-monitoring-all`: the SIP gateway is considered as down when all the dial-peer VoIP linked to the SIP gateway are down.

Use the following command to make the status of the SIP gateway follow the status of the voice ports (the reverse of the previous command). For example: to have the SIP gateway de-registered when all physical ports are down.

```
CLI(sipgw)> [no] intrusive-voiceport { atm-if-status
| sip-gateway-if-status | registration-status | registration-error
| port-registration-error | sip-monitoring | sip-monitoring-all }
{ and-mode | or-mode } [<5/u,5/v,5/w,voip/x,voip/y,voip/z>]
```

- Impact of the voice port status on the SIP gateway status: `and-mode` means that all the specified ports must be up for the gateway is up (the gateway is down if at least one the specified ports is down); `or-mode` means that all the specified ports must be down for the gateway is down (the gateway is up if at least one of the specified ports is up).
- Refer to the previous command for the signification of other parameters.

Use the following command to make the status of the voice ports follow the status of the SIP gateway and vice versa to make the status of the SIP gateway follow the status of the voice ports (the behavior of the two previous commands).

```
CLI(sipgw)> [no] intrusive-voiceport both-way { atm-if-status
| sip-gateway-if-status | registration-status | registration-error
| port-registration-error | sip-monitoring | sip-monitoring-all }
{ and-mode | or-mode } [<5/u,5/v,5/w,voip/x,voip/y,voip/z>]
```

- `both-way` forces a bi-directional intrusive mode. If SIP gateway is down, the list of voice ports is set down and if the list of voice ports is not up, the SIP gateway is set down.
- Refer to the two previous commands for the signification of other parameters.

6.7.7 Number portability

Use the following command to force the state of the number portability function. The timeout parameter is optional and specifies the duration of the "in-progress" state. The default value is 5760 minutes (4 days). Use the no form to disable the portability function (default).

```
CLI(sipgw)> [no] set-portability { enable | in-progress | done }
                                    [timeout <time-in-minutes 1-525600>]
```

6.8 VOIP CODER PROFILES CONFIGURATION

It is possible to define a list of coders for the terminal capabilities. The list contains the preference order, in which the codec shall be used when negotiating the codec with the remote VoIP endpoint.

Commands:

```
CLI(configure)> voip-coder-profile 1
CLI(voip-coder)> codec 1 g726r32 30
CLI(voip-coder)> codec 2 g729ab 10
```

Parameters:

```
CLI(voip-coder)> codec <preference-index> <codec> [<sample-time-length>]
                                                  [rtp-dynamic <96-127>]
```

- `preference index`: indicates the position in the list of coders (1 to 10).
- `codec`: may be g729ab, g711a, g711u, g726r32.
- `sample-time-length`: period of frames transmission (in ms). Allowed values are:
  - `g729ab`: 10, 20, 30, 40. Default: 20. If G.729AB is configured and SIP is the VoIP protocol, the codec in SDP indicates G.729 (`rtpmap=18 (G729)`, whereas the media is G.729AB or G.729A, which are compatible codecs).
  - `g711a, g711u`: 10, 20, 30, 40. Default: 20.
  - `g726r32`: 10, 20, 30, 40. Default: 20.
- `rtp-dynamic <96..127>`: relevant for SIP only. Allows defining dynamic payload types. Some checks with other payload types configured for DTMF and UDI64K are done. If the `rtp-dynamic` option is absent, the standard payload type values are used.

Note: G723.1 is not available in the standard OneOS software.

The selected coder will be the first one in the list matching with the remote capabilities.

6.9 VOICE OVER IP DIAL PEER CONFIGURATION

The VoIP port is defined as a "Voice over IP Dial Peer", that identifies the remote H.323/SIP devices which can enter in communication with the OneOS-based voice-capable router.

Voice over IP dial peers must be created to define all the parameters related to the remote H.323/SIP devices.

For outbound calls, the peer is selected in the routing table. A single peer can be defined for several remote devices when using a H.323 Gatekeeper or a SIP proxy.

For inbound calls, the OneOS-based voice-capable router tries to identify the caller using its IP source address (compared with the IP address configured in the dial-peer VoIP). If it is not found, the parameters specified in the first configured dial-peer are used.

To create a dial-peer VoIP, enter:

```
CLI(configure)> dial-peer voice voip <index 0-7>
CLI(voip)>
```

One can create several VoIP dial peers; therefore, an arbitrary number (index) identifies each dial peer.

6.9.1 Common Parameters

Use the following command to define the voice coder profile to use with the dial-peer. The profile is identified by a number from 0 to 7 (see 6.8). Default: 0. When no coder profile is defined, the G.711A/20ms coder is used.

```
CLI(voip)> voip-coder-profile < 0-7>
```

Use the following command to disable the packet loss concealment (PLC) algorithms with G.711. Default: not disabled.

```
CLI(voip)> no g711-plc
```

Use the following command to use preferably the G.729 (resp. G.729B) codec instead of the G.729A (resp. G.729AB) codec if there is enough bandwidth available. In case of lack of bandwidth the calls are switched back to G.729A (resp. G.729AB) codec.

```
CLI(voip)> [no] g729-dynamic
```

Note: this command is not available on all the ONE range of products. The use on an OneOS-based voice-capable router that does not implement this command results in the "Command not supported on this device…" error message.

Use the following command to enable the silence detection and suppression. Use `vad` for standard voice activity detection. The value `vadcng` can be used for G.711 and G.726 to enable the comfort noise generation (this feature is de-facto enabled if `vad` is configured with G.729AB). Use the `no` form to disable the voice activity detection. Default: disable.

```
CLI(voip)> [no] silence-detection { vad | vadcng }
```

Use the following command to specify the fax management mode.

```
CLI(voip)> [no] fax-relay { passthrough | t38 | t38orpassthrough
                          | t38nse | t38andvoice }
                          [priority { t38 | passthrough }]
                          [requested { simultaneously | successively }]
```

- passthrough: in this mode the media is forced to G.711 (codec up-speed mode).
- t38: in this mode the media is forced to T.38.
- t38orpassthrough: in this mode T.38 and modem pass-through as possible media capabilities. If the remote gateway does not support T.38, the capabilities are negotiated such that modem pass-trough is used instead of T.38.
- t38nse: in this mode the media is switched to T.38 by sending a set of RTP frames called NSE (Named Service Event). This mode is not standard compliant, but enables interoperability with Cisco gateways when a similar mode is configured on Cisco gateways.
- t38andvoice: in this mode T.38 and G.711 pass-through are used simultaneously. This mode is not standard compliant, but enables interoperability with certain gateways working that way.
- priority: if the remote gateway supports T.38 and G.711 pass-through, then the priority parameter defines the mode to apply (default priority: t38).
- requested: if the remote gateway supports T.38 and G.711 pass-through, then the requested parameter defines if the two modes are tried simultaneously (default) or successively.

Use the no form to suppress the fax management.

Use the following command to specify the G3 FAX detection criterion.

```
CLI(voip)> detection-fax { flagV21 | CED }
```

- flagV21: in this mode the FAX is detected when the V.21 flags are received. This mode is more reliable but may increase, in some cases, the connection time (default).
- CED: in this mode the FAX is detected as soon as a CED tone is detected. It should not be configured in CED mode if low speed modems are used (such a modem sends also CED tones and will be then interpreted as a fax call instead of a modem call).

Use the following command to specify the number of T.38 frames added for redundancy. Default: 0.

```
CLI(voip)> [no] t38-redundancy <0-4>
```

Note that adding frames for redundancy can increase a lot (up to 5 times) the needed bitrate, especially for high rate modulations. Provision has been taken, according to the following table, to avoid such drawback.

T38-redundancy	V.21	V.27 2400	V.27 4800	V29. 7200	V.29 9600	V.17 12000	V.17 14400
0	3	0	0	0	0	0	0
1	4	2	1	1	1	1	1
2	4	4	3	2	2	2	2
3	4	4	4	3	3	3	3
4	4	4	4	4	4	3	3

Use the no form to suppress redundancy.

Use the following command to enable or disable the ECM (Error Correction Mode). The ECM divides fax pages in HDLC frames so that transmission errors are detected by means of a CRC check. When the remote fax receives a full page, it identifies frames with wrong CRC and requests the sending fax to retransmit these frames. The process is repeated until all frames are received without CRC errors. In case of a noisy fax reception (i.e. with CRC errors), the ECM enables a high quality fax transmission.

```
CLI(voip)> t38-ecm { enable | disable }
```

enabled is the default value. As ECM was not supported in former OneOS versions, in case of fax transmission problems when upgrading to a newer version, it can be interesting to compare results with disabled ECM.

Use the following command to limit the rate of the fax-relay. When the rate is 7200 bps the first training at 9600 bps is corrupted to force a fallback to 7200 bps. Default: 9600. It means that 14.4 kbps V.17 fax will connect at 9.6 kbps by default. To allow V.17 fax, use "t38-rate 14400".

```
CLI(voip)> t38-rate { 4800 | 7200 | 9600 | 14400 }
```

Use the following command to install a timer (in seconds) in order to avoid the switch in T.38 mode when detecting a fax-modem tone. In that case, the detection is done only during the time defined by the timer. This feature can be enabled if some wrong fax detections are observed during voice calls. Use the no form to remove the timer (default).

```
CLI(voip)> [no] timer-max-detection <1..120>
```

Use the following command to enable or disable the fallback of Fax Super G.3 to Fax G.3 when the pass through mode is not allowed in order to send the fax with T.38 protocol. When enable the tone “ANSam” of the fax Super G.3 is replaced by a command T.38 CED of a G.3 fax. If the voice codec is G.711 or the T.38 mode not negotiated, the function is disabled. Disable is the default value.

```
CLI(voip)> sg3tog3 { enable | disable } [<timer:100-3000ms>]
```

timer:100-3000ms is a configurable timer that defines the maximum time allowed to receive the CNG tone (from the calling FAX) at the beginning of the call. It avoids wrong detections and voice cuts due to ANSam tone suppression during the call (given in ms in 100ms steps; default value: 1000 = 1 sec).

Use the following command to enable the automatic modem detection. Use the no form to disable the modem detection. The method used for up-speed G.711 is defined by the passthrough-mode command.

```
CLI(voip)> [no] modem-passthrough
```

Use the following command to switch automatically to G.711 if the received flow switches to G.711. This parameter must be set to enable if the remote device switches directly to G.711 without sending NSE RTP packets before. Default: disable.

```
CLI(voip)> passthrough-symetric { enable | disable }
```

Use the following command to specify the codec to be used in modem/fax pass through mode (up-speed to G.711). Default: G.711A.

```
CLI(voip)> passthrough-codec { g711a | g711u }
```

Use the following command to specify the jitter max value for voice (in ms). Default: 100ms.

```
CLI(voip)> [no] jitter <20..1000>
```

Use the following command to eventually specify a different jitter max value for fax (in ms). Default: 100ms.

```
CLI(voip)> fax-jitter <20..1000>
```

Use the following command to

```
CLI(voip)> jitter-compensation { fixed | adaptive }
```

Use the following command to enable the implicit routing. All the incoming calls are routed to the specified destination whatever the destination number is. Use the no form to disable the implicit routing.

```
CLI(voip)> [no] implicit-routing { pots | pots-group | voice-group
                                 | voip | voip-group } <identifier>
```

Use the following command to specify the emergency level for any call arriving on this port. Default: 100.

```
CLI(voip)> emergency <1..200>
```

Use the following command to select the type of user-to-user service (UUS) supported by the port. When a specific service is not configured, UUS Information Elements are stripped from the ISDN message before forwarding process (default: service 1 – UUS1):

```
CLI(voip)> [no] ie-uui [service { 1 | 2 | 3 | 1&2 | 1&3 | 2&3 | 1to3 }]
```

Use the following command to specify the coding rule used for the information element containing the Advice of Charge (AOC) information. Default: ETSI. Use the optional parameter AOC-E generation to have the charging information being computed by the OneOS-based router (available only for H.323).

```
CLI(voip)> [no] aoc-format { etsi | ecma | sip-aoc99-tls }
                           [aoc-e-generation { local | remote }]
```

Use the following command to limit the number of active call sessions with the defined destination. Default: 32 (default value is 300 on ONE300).

```
CLI(voip)> max-conn <0..32>
```

Use the following command to define the Q.850 cause value when `max-conn` is exceeded (default 47).

```
CLI(voip)> max-conn-q850cause <cause>
```

Use the following command to enable RTCP-XR frames for MOS calculation. As of V4.2R4 software release, RTCP-XR is enabled by default. Prior to that release, RTCP-XR is disabled by default.

```
CLI(voip)> [no] rtcp-xr
```

Use the following command to select the signaling protocol to use. Default: h323.

```
CLI(voip)> sig-protocol { h323 | sip | mgcp }
```

VoIP dial-peers may be grouped as in a `voip-group` in an analog way as pots-group. Several VoIP dial-peers are member of a `voip-group` if they have the same `voip-group` number. Then, it becomes possible to route calls to a `voip-group`. OneOS voice-routing distributes the call over the various dial-peers that are member of the group. To configure the `voip-group`:

```
CLI(voip)> [no] voip-group <id:0-30> [priority <0-30>]
```

VoIP dial-peers may be grouped in a voice group. A voice group can contain POTS and VoIP ports. To configure the `voice-group`:

```
CLI(voip)> [no] voice-group <id:0-30> [priority <0-30>]
```

Use the following command to define the default priority of the port in the group (if not defined in the `voip-group` or `voice-group` command). In the group all the interfaces with the same priority are selected circularly (round robin) or according to the load (load balancing). Default: 0.

```
CLI(voip)> [no] priority <0..30>
```

The following commands are used for the routing process. They are described in the corresponding chapter (see 7.2).

```
CLI(voip)> default-type-of-number

CLI(voip)> numplan-preprocessing

CLI(voip)> international-numplan

CLI(voip)> national-numplan
```

To disable the dial peer voice VoIP, use the following command. Use `no shutdown` to re-enable the dial peer voice VoIP (default).

```
CLI(voip)> [no] shutdown
```

6.9.2 SIP-Specific Parameters

Use the following command to tell that the peer is a SIP user agent (server or proxy).

```
CLI(voip)> sig-protocol sip
```

Use the following command to link the dial-peer VoIP to the SIP server. See 9.2.2 for more details. Use the no form of the command to remove the link.

```
CLI(voip)> sip-ua { ip-dynamic [restricted | open]
                  | ip-static <A.B.C.D> | mac-static <aa:bb:cc:dd:ee:ff> }

CLI(voip)> no sip-ua
```

Use the following command to specify the gateway address (syntax: A.B.C.D:<port> or host:<port>). It must be specified if a SIP proxy is not configured under the sip-gateway. It is optional if a proxy is already declared and it overrides the default proxy configured under sip-gateway. The optional via parameters specifies an outbound proxy for all the signaling messages. Use the no form of the command to remove the gateway.

```
CLI(voip)> gw-ip-address <IP-address>[:<port>] [via <IP-address>]

CLI(voip)> no gw-ip-address
```

Use the following command to allow sending and processing SDP information in 180 Ringing messages. It makes it possible to send and/or receive ringback tones through the RTP flow. Send AND receive is the default value. Please refer to 5.1.7 for more details. Use the no form of the command to disallow.

```
CLI(voip)> sip-sdp-on-alert [send-receive | receive-only | send-only]

CLI(voip)> no sip-sdp-on-alert
```

When SDP sending is allowed, the ringback tone is played immediately from the received RTP flow. It might happen that the RTP stream does come immediately after that the in-band IE is sent on the ISDN interface. Use the following command so that an in-band IE is sent in a message from VoIP to pots only after a first RTP packet is received. Use the no form of the command to remove this configuration.

```
CLI(voip)> rtp-inband-notification

CLI(voip)> no rtp-inband-notification
```

Use the following command for SIP proxies requiring PRACK messages. PRACK messages are sent by the OneOS-based voice-capable router when provisional answers (trying, ringing, etc…) are received. Use the optional parameter to avoid sending offer in PRACK message if offer has been already sent. Use the no form of the command to avoid sending PRACK messages (default).

```
CLI(voip)> force-prack [no-additional-offer]

CLI(voip)> no force-prack
```

Use the following command to avoid sending offer in INVITE message if offer has been already sent.

```
CLI(voip)> no-additional-offer in-invite-200
```

Use the following command to allow sending offer in INVITE message although offer has been already sent (default).

```
CLI(voip)> no-additional-offer deactivated
```

Use the following command to define the behavior for ending the fork process. Either the fork process is ended in the gateway (default: cancel) or locally if the gateway is not able to end the process (no-cancel).

```
CLI(voip)> fork-stop { cancel | no-cancel }
```

Use the following command to define how the codec is chosen when receiving a call. If local (default value): the selected codec is the first local codec that is the same as one of the remote codec(s). If remote: the selected codec is the first remote codec that is the same as one of the local codec(s). Use the no form of the command to return to the default value.

```
CLI(voip)> coder-selection-priority { remote | local }

CLI(voip)> no coder-selection-priority
```

Use the following command to send RTP silence frames instead of none in order to maintain NAT sessions (Hosted Nat Transversal) when a call is typically in hold state with valid SDP IP address. Use the no form of the command to stop sending RTP silence frames.

```
CLI(voip)> rtp-permanent

CLI(voip)> no rtp-permanent
```

Use the following command to enable the SIP trunking mode on the dial peer. For outbound INVITE message, a P-Preferred-Identity header is added with the defined name and there is only one Registration session for the trunk (the routing table is not checked for multiple registrations). Default: disable. Use the no form of the command to return to default.

```
CLI(voip)> trunking-mode p-preferred-id <id: 1-120 char>

CLI(voip)> no trunking-mode
```

Use the following command to specify if the hostname (if configured) or the IP address or the URI contact parameter of the SIP gateway (default) must be used in the "Contact" header field.

```
CLI(voip)> uri-contact { hostname | ip-address | default }
```

Use the following command to specify that the calling information must be inserted into the "P-Preferred-Id" header field. Use the no form of the command to not insert the calling information into the "P-Preferred-Id" header field.

```
CLI(voip)> sip-preferred-id

CLI(voip)> no sip-preferred-id
```

Use the following command to specify that the calling information must be inserted into the "P-Asserted-Id" header field. Use the no form of the command to not insert the calling information into the "P-Asserted-Id" header field.

```
CLI(voip)> sip-asserted-id

CLI(voip)> no sip-asserted-id
```

Use the following command to force SIP FROM IE (information element) value into message when this information (calling number) is not present even after voice-routing mechanism is achieved. Otherwise by default, when calling number is empty, FROM IE is set with sip-gateway.sip-username or sip-server.sip-username parameter depending on the direction of the call (default value). Use the no form of the command to return to the default value.

```
CLI(voip)> sip-default-from <string up to 50 char>

CLI(voip)> no sip-default-from
```

Use the following command to force the SIP privacy header to the chosen value (for SIP outgoing calls only). Possible values are user (RFC3323), ID (RFC3325) or both. Use the no form of the command to return to the default value: ID (RFC3325).

```
CLI(voip)> sip-privacy-header { user | id | user-id }
```

Use the following command to modify the default mapping of SIP release causes into ISDN release causes. Use the no form of the command to return to the default mapping (described in 4.1.6). Note that following message "Warning: This sip cause (xxx) is not supported." Is displayed when the requested SIP release cause is not taken into account by the OneOS-based router.

```
CLI(voip)> sip-to-isdn-cause <sip-cause:400-606> <isdn-cause:1-127>

CLI(voip)> no sip-to-isdn-cause <sip-cause:400-606>
```

Use the following command to modify the default mapping of SIP no response cause into ISDN release cause. Cause 127 is the default mapping.

```
CLI(voip)> q850-cause-on-no-response <isdn-cause:1-127>
```

Use the following command to have the first SIP INVITE-183 message being transformed into ISDN ALERTING message. Use the no form of the command to return to the default behavior (not transformed).

```
CLI(voip)> sip-183-alerting

CLI(voip)> no sip-183-alerting
```

Use the following command to define how to carry AOC information through SIP network.

```
CLI(voip)> sip-aoc-ie { generic-cpk | generic | xml | raw }
```

generic-cpk is used to carry AOC information in "application/vnd.cirpack.isdn-ext" MIME type by creating ISDN raw data in SIP MIME body (default value).

Generic is used to carry AOC information in "application/vnd.isdn.aoc" MIME type by creating ISDN raw data in SIP MIME body.

Xml is used to carry AOC information in "application/vnd.etsi.aoc+xml" MIME type according to 3GPP TS 24.647 Advice Of Charge (AOC) using IP Multimedia (IM) Core Network (CN) subsystem.

Raw is used to carry AOC information in "application/vnd.oneaccess.isdn.aoc-ext" MIME type by creating full ISDN raw data in SIP MIME body (including facility IE header).

Use the following command to define how to carry User-to-User information through SIP network.

```
CLI(voip)> sip-uus-ie { user-to-user | mime }
```

Refer to 4.2.5.2 for more information (user-to-user is the default value).

Use the following command to define how to translate ISDN numbering headers to and from SIP messages using the "phone-context" header (according to ETS TS 183 036). This feature applies only for dialog generated messages. It covers the following SIP Information Elements: Request-URI, From, To, P-Asserted-Identity, P-Preferred-Identity and Contact.

```
CLI(voip)> sip-phone-context <name> { unknown | national
                                    | international | all }
```

name is the string of 20 characters at most that will translate the given ISDN type of number. Use all to have the string used for any ISDN type of number. Note that this command can be used several times.

Use the no form of the command to remove the feature.

```
CLI(voip)> no sip-phone-context { unknown | national | international
                                                    | [all] }
```

In case the dial-peer is an IP-PBX, it might be interesting to monitor its status by sending (send – default value) or receiving (receive) periodically (60 seconds by default) SIP messages (method – OPTIONS message by default). As long as periodic messages are acknowledged, calls can be routed to that dial-peer. If the dial-peer is not of type sip-ua (i.e. the dial-peer defines the VoIP peer for the telecom operator's SIP platform) and SIP monitoring is active, the OPTIONS message can be sent or received to probe that the remote SIP platform is reachable. When all dial-peers not of type sip-ua are down because of SIP monitoring, INVITE and REGISTER from SIP proxy are managed in backup mode. INVITE is routed to another local port and REGISTER is handled locally by the SIP server. Use the following command to active dial-peer monitoring. Use the no form of the command to deactivate dial-peer monitoring (default).

```
CLI(voip)> sip-monitoring [<method>] [send | receive] <3..600 seconds>

CLI(voip)> no sip-monitoring
```

Use the following command to specify the method to be applied for down-speed to G.729 in case of bandwidth lack.

```
CLI(voip)> voice-coder-negotiation { direct | reinvite }
```

- direct: It is the default value. No changeover is done.
- reinvite: the codec change is re-negotiated by sending RE-INVITE message. Note that this method is mandatory to have the call admission control working (see 10).

Use the following command to specify the method to be applied for up-speed to G.711 in case of Modem & FAX detection.

```
CLI(voip)> passthrough-mode { direct | reinvite }
```

- direct: proprietary method, which consists in switching directly to G.711 the RTP flow without any signaling process (specific NSE RTP packets are sent before switching). It is the default value.
- reinvite: the codec change is re-negotiated by sending RE-INVITE message.

Use the following command to specify the DTMF management mode.

```
CLI(voip)> dtmf-relay { in-band | sip-info | in-band-or-sip-info }
           [forced | depend-of-remote] [<payload-type:96-127>]
           [payload-asymmetric | payload-symmetric]
```

- in-band: DTMF codes are transmitted in RTP frames (RFC 2833).
- sip-info: (default) DTMF codes are sent to the remote user agent/proxy/gateway via SIP INFO messages.
- in-band-or-sip-info: DTMF codes are sent according to the remote capability.
- forced: DTMF codes are sent to remote and do not take into account the remote capabilities (only with in-band mode).
- depend-of-remote: DTMF codes are sent by default to the remote only if the remote peer indicates in SDP if it can receive DTMF (SDP line containing fmtp string).
- <payload-type:96-127>: the payload type for DTMF can be specified (default 101).

- payload-asymmetric: the DTMF is sent to remote according to the remote capacities, and the DTMF is received according to the programming.
- payload-symmetric: the DTMF is sent to remote and received according to the first offer (remote capacities or programming).

Use the no form of the command to suppress the DTMF management.

```
CLI(voip)> no dtmf-relay
```

Use the following command to specify the flash management mode.

```
CLI(voip)> flash-relay { sip-info | in-band }
```

- sip-info: (default) flash is sent to the remote user agent/proxy/gateway via SIP INFO messages.
- in-band: flash is transmitted in RTP frames (RFC 2833).

Use the no form of the command to suppress the flash management.

```
CLI(voip)> no flash-relay
```

Use the following command to specify the ISDN to DIP overlap method.

```
CLI(voip)> sip-overlap-type { rfc3578 | zhang-overlap }
```

- rfc3578: (default) overlap dialing is transmitted according to RFC 3578.
- zhang-overlap: overlap dialing is transmitted according to draft-zhang-sipping-overlap.

Use the no form of the command to return to the default value.

```
CLI(voip)> no sip-overlap-type
```

6.9.3 H.323-Specific Parameters

Use the following command to tell that the signaling protocol is H.323.

```
CLI(voip)> sig-protocol h323
```

Use the following command to define if a gatekeeper must be registered and available to establish the call (mandatory) or if the routing table routes the calls when there are no gatekeeper available (optional, default value). Use the no form of the command to return to the default value.

```
CLI(voip)> [no] gatekeeper { optional | mandatory }
```

```
CLI(voip)> no gatekeeper
```

Use the following command to specify the gateway address. It must be specified if a gatekeeper is not used or is optional, unless the IP address is directly configured in the routing table. Use the no form of the command to remove the gateway address.

```
CLI(voip)> gw-ip-address { <IP-address>|<host-name> }[:<port>]
```

```
CLI(voip)> no gw-ip-address
```

Use the following command to enable the H.323 fast-connect mode. If start-h245 is configured, the OneOS-based voice-capable router will send a Facility message with a "start H245" command upon an incoming call, if capabilities requiring H245 are enabled (T38 FAX, DTMF out of band, and Analog interface for hook flash). If no-t38 is configured, T38 will be removed from the Facility message. Default: fast-connect no-start-h245 t38). Use the no form of the command to disable fast-connect mode.

```
CLI(voip)> fast-connect [start-h245 | no-start-h245] [no-t38 | t38]
```

```
CLI(voip)> no fast-connect
```

Use the following command to enable the h245 tunneling mode. Use the no form of the command to disable the tunneling mode (default value).

```
CLI(voip)> h245-tunnel

CLI(voip)> no h245-tunnel
```

Use the following command to enable a mode where any failure on the media channel opening has no effect on the call signaling. If enable, a call can remain established without any RTP flow (no voice). In this case, the call must be disconnected by the users. Use the no form of the command to disable (default).

```
CLI(voip)> call-media-independent

CLI(voip)> no call-media-independent
```

Use the following command to insert (to force) a PROGRESS Information Element “Inband information” in Alert message coming from the H.323 remote end. It enables the process of the received RTP flow for the call back tone. Use the no form of the command to not insert (default).

```
CLI(voip)> force-rec-inband

CLI(voip)> no force-rec-inband
```

Use the following command to insert a PROGRESS Information element “Inband information” in Alert message sent from ISDN to other protocols (H.323, SIP, ISDN and FXS). It may be necessary to ask the remote end to take into account the RTP flow sent before connection (ringback tone, for example).Use the no form of the command to not insert (default).

```
CLI(voip)> force-tx-inband

CLI(voip)> no force-tx-inband
```

Use the following command to remove the PROGRESS Information element “Inband information” in Alert message sent from ISDN to other protocols (H.323, SIP, ISDN and FXS). Use the no form of the command to not remove (default).

```
CLI(voip)> suppress-tx-inband

CLI(voip)> no suppress-tx-inband
```

Use the following command to specify the method to be applied for down-speed to G.729 in case of bandwidth lack.

```
CLI(voip)> voice-coder-negotiation { direct | request-mode | tcsnull }
```

- direct: It is the default value. No changeover is done.
- request-mode: standardized method using the h245 Request-Mode message to force the remote peer to switch.
- tcsnull: standardized method using the h245 capabilities renegotiation with a coder restriction.

Use the following command to specify the method to be applied for up-speed to G.711 in case of Modem & FAX detection.

```
CLI(voip)> passthrough-mode { direct | request-mode | tcsnull }
```

- `direct`: proprietary method, which consists in switching directly to G.711 the RTP flow without any h245 signaling process (specific NSE RTP packets are sent before switching). It is the default value.
- `request-mode`: standardized method using the h245 Request-Mode message to force the remote peer to switch to G.711.
- `tcsnull`: standardized method using the h245 capabilities renegotiation with a restriction to G.711.

Use the following command to specify the DTMF management mode.

```
CLI(voip)> dtmf-relay { h245alpha | h245signal | in-band }
                      [forced | depend-of-remote] [<payload-type:96-127>]
                      [payload-asymmetric | payload-symmetric]
```

- `h245alpha`: DTMF codes are sent using H.245 in alphanumeric format (default).
- `h245signal`: DTMF codes are sent using H.245 signal.
- `in-band`: DTMF codes are transmitted in RTP frames (RFC 2833).
- `forced`: DTMF codes are sent to remote and do not take into account the remote capabilities (only with `in-band` mode).
- `depend-of-remote`: DTMF codes are sent by default to the remote only if the remote peer indicates in SDP if it can receive DTMF (SDP line containing `fmtp` string).
- `<payload-type:96-127>`: the payload type for DTMF can be specified (default 101).
- `payload-asymmetric`: the DTMF is sent to remote according to the remote capacities, and the DTMF is received according to the programming.
- `payload-symmetric`: the DTMF is sent to remote and received according to the first offer (remote capacities or programming).

Use the `no` form of the command to suppress the DTMF management.

```
CLI(voip)> no dtmf-relay
```

7 VOICE OVER IP ROUTING TABLE

7.1 VOIP ROUTING OVERVIEW

7.1.1 Introduction

Voice call routing is a key element to apply modifications on received calls and is intended for several purposes:

- Simple call routing when no gatekeeper is declared.
- Insertion and suppression of prefixes/suffixes in the called/calling numbers.
- Force the use of some types of codec/bearer capabilities for some applications where fax/modem transport over IP is required, flexibility is required to achieve interoperability with gateways having fewer features.
- Voice call backup in case of network failure.

Incoming calls are matches against a list of number patterns; if the called number matches a pattern, then the configured transformations and routing are applied.

The following sections will focus on a more detailed description of routing.

7.1.2 Numbering plan management and routing process

In order to make the routing table as simple as possible – routing the calls without handling the numbering plan prefixes (national, international, country code) – OneOS provides functions to describe the numbering plan and to process the numbers with regard to that numbering plan before (pre-processing) and after (post-processing) the routing process. It is possible to check a specific numbering plan type with a number or prefix defined in the routing table. It is also possible to force a numbering plan value for the called or calling number (see the routing table configuration).

7.1.3 Dial plan management

When working with an open numbering plan that features variance in length of number, `timer` or `timer-or-#` have to be selected in the routing table to consider the dialing completed.

Instead of relying only on timers to consider the dialing completed, it is possible to use a digit map that describes the various lengths of number according to the dialing plan.

When an incoming call (overlap or en-bloc) is received from the POTS (FXS or ISDN), it is parsed against the digit map. When it matches a described dialing number, the call is processed through voice routing like an en-bloc dialed call. The matching to the dial plan depends on:

- The type of the called (dialed) number (international or not).
- The presence or not of the file that describes the dial plan.
- The application of the dial plan (no or mandatory or optional).
- The presence or not of the end of dialing indication (elapsed timer or sending complete IE).

The following table shows how the call is processed in the various cases.

Type of called number	Dial plan file presence	Dial plan application	End of dialing indication	Result of the parsing	Resulting action
international	indifferent	indifferent	indifferent	not parsed	voice routing
indifferent	indifferent	no	indifferent	not parsed	voice routing
not international	no	optional	indifferent	not parsed	voice routing
not international	no	mandatory	indifferent	not parsed	disconnection
not international	yes	mandatory or optional	indifferent	total match	voice routing (with en-bloc)
not international	yes	optional	indifferent	no match	voice routing
not international	yes	mandatory	indifferent	no match	disconnection
not international	yes	mandatory or optional	no	partial match	wait for more digits
not international	yes	optional	yes	partial match	voice routing
not international	yes	mandatory	yes	partial match	disconnection

7.1.4 Wildcards

Prior to achieve number matching against a prefix in the routing table, you might need to define wildcards.

Wildcard "any number": It is referenced as the dot character "**.**". When you write a prefix with this wild card, the dot represents any number of any lengths. In the following example: "10**.**" Stands for 10….

Wildcard "any digit": It is referenced as the X character "**X**". When you write a prefix with this wild card, the X represents any digit character. In the following example: "10**X**" stands for 100 to 109, 10***** and 10#.

Wildcards "digit subset": They are referenced as a letter such as "A", "B", "C" … (except "X"). When you write a prefix with such wild card, the letter represents any of the configured digits. In the following example: "wildcard C 01234" the letter C stands for 0 or 1 or 2 or 3 or 4.

See examples using wildcards at the end of the next chapter.

Note: Wildcards and Regular expressions (see below) are exclusives.

7.1.5 Regular expressions

Another way to define number matching criteria in the routing table is to use regular expressions that are a more powerful tool than the wildcards described above (the OneOS regular expressions implementation is based on POSIX Extended Regular Expressions; character classes are not accepted).

Note: Regular expressions and Wildcards (see above) are exclusives.

The available syntax for number matching using regular expressions is described in the following table. In the table "digit" stands for 0-9, # and *****; because ***** is used by the syntax, as a digit it must be noted **[*]**.

Syntax	Meaning

`[ ]`
`Ex.: [123]`
`Ex.: [2-8]`
	Defines any single digit that is inside the brackets.
	Means 1, 2, 3 and nothing else.
	Means any single digit between 2 and 8 (i.e. 2, 3, 4, 5, 6, 7, 8).

`[^ ]`
`Ex.: [^123]`
`Ex.: [^2-8]`
	Defines any single digit that is not inside the brackets.
	Means any single digit except 1, 2, 3.
	Means any single digit that is not between 2 and 8 (i.e. 0, 1, 9, #, *).

`. (dot)` `Ex.: 0.0`	Defines any single digit. Means 000, 010, 020 … 090, 0#0, 0*0.

`* (star)`
`Ex.: 12*3`
`Ex.: [12]*3`
	Defines the preceding digit zero or more times.
	Means 13, 123, 1223, 12223, etc.
	Means 3, 13, 23, 113, 123, 213, 223, 1113 … 2222121223, etc.

`+ (plus)`
`Ex.: 12+3`
`Ex.: [12]+3`
	Defines the preceding digit one or more times.
	Means 123, 1223, 12223, etc.
	Means 13, 23, 113, 123, 213, 223, 1113 … 2222121223, etc.

`? (question mark)`
`Ex.: 12?3`
`Ex.: [12]?3`
	Defines the preceding digit zero or one time.
	Means 13, 123.
	Means 3, 13, 23.

`{m,n}` `Ex.: 1{3,5}`	Defines the preceding digit at least m times and not more than n times. Means 111, 1111, 11111
`^ (circumflex)` `Ex.: ^0`	Defines the starting position within the number. Means any number starting with 0.
`$ (dollar sign)` `Ex.: 0$`	Defines the ending position within the number. Means any number ending in 0.
`| (pipe)` `Ex.: 123|456`	Defines a choice. Means 123 or 456.
`( )`	Defines a sub-expression that is part of an expression.

Examples of prefix matching with regular expressions and wildcards:

Regular expression	Wildcards	Prefix matching
`^0141877400$`	`0141877400`	Exact match with 0141877400
`^014187.{4,4}$ or ^014187....$`	`014187.` `length 10`	Match any 10-digit long number starting with 014187
`^014187740.$`	`014187740X`	Match any 10-digit long number starting with 01418740
`^014187[789]...$`	`014187AXXX` `with A=789`	Match any 10-digit long number starting with 0141877 or 0141878 or 0141879
`70(0[0-9]|[1-7][0-9]|80)$`	`.7000 to .7080`	Match any number ending in the range 7000 to 7080
`^[*]67#$`	`*67#`	Exact match with *67#
`^014187[^0]...$`	`014187AXXX` `with A=123456789`	Match any 10-digit long number starting with 014187 except those starting with 0141870
`^014187`	`014187.`	Match any number of any length starting with 014187 (use timer-or-#)
`^$`	`-`	Empty number
`^ or $ or [0-9*#]{0,35}`	`.`	Any number including empty number
`[0-9*#]+`	`X or . length 1`	Any number not empty

7.1.6 Routing process summary

7.1.6.1 Case of a call coming from a local port

The routing has the following general structure:

Incoming call routing and transformation → Translation → Routing → Outgoing routing

1. The calling number translation defined in the dial-peer voice pots is applied.
2. The routing table is checked against the incoming routing rules (with prefix-type = incoming or in-and-out) according to the configured number type (calling or called) and with the dial-peer = pots-group corresponding to the local port.
3. If a match is found, translations on calling and/or called numbers are applied. If `reject` is configured, the call is cleared. If `next` is configured, the routing table is checked again from the specified rule with the translated numbers. If a match is found, translations on calling & called numbers are applied again. This process is applied until the end of the table or until a `last` option is encountered. This process enables several number translations.
4. The implicit-routing parameter of the dial-peer pots is checked. If defined, the call is directly routed to the corresponding VoIP peer (dial-peer VoIP) or local port (dial-peer POTS). The routing process is completed.
5. The routing table is checked (from the first rule) against the outgoing rules (prefix-type = outgoing or in-and-out) according to the number type (calling or called).
6. Upon a total match, translations on calling and/or called numbers are applied and the call is routed to the dial-peer VoIP port. The routing process is finished. It will be restarted from this step in case of `backup` (and go to step 5 from the following routing rule).
7. Upon a partial match (in case of overlap dialing only), the routing is considered inconclusive but the second end-of-dialing timer is started. The routing process will be done again with the following digit or upon the second end-of-dialing timer expiry.
8. If no match, the call is cleared.

7.1.6.2 Case of a call coming from the H.323/SIP Network

1. The routing table is checked against the incoming routing rules (with prefix-type = incoming or in-and-out) according to the configured number type (calling or called) and with the dial-peer = VoIP. In this step, the dial-per VoIP identifier is unknown.
2. Upon a match, the dial-peer VoIP identifier is taken into account to determine for example a voice coding profile. Translations on calling and/or called numbers are applied. If `reject` is configured, the call is cleared. If `next` is configured, the routing table is checked again from the specified rule with the translated numbers. Upon a match, translations on calling & called numbers are applied again. This process is applied until the end of the table or until a `last` option is encountered. Then go directly to step 4.
3. If no match, the source IP address is compared to the address configured in all the dial-peer VoIP. In case of match, the corresponding dial-peer VoIP is selected. If not, the lowest dial-peer VoIP identifier is selected by default.
4. The implicit-routing parameter of the selected dial-peer VoIP is checked. If defined, the call is directly routed to the corresponding pots-group. The routing process is finished.
5. The routing table is checked (from the first rule) against the outgoing rules (prefix-type = outgoing or in-and-out) according to the number type (calling or called) and with dial-peer = pots-group.
6. Upon a total match, translations on calling and/or called numbers are applied and the call is routed to the dial-peer pots-group. The routing process is finished. It will be restarted from this step in case of `backup` (and go to step 5 from the following routing rule).
7. Upon a partial match (in case of overlap dialing only), the routing is considered inconclusive and the second end-of-dialing timer is started. All the routing process will be done again with the fully received number when the following digit will be received or when the second end-of-dialing timer will elapse.
8. If no match, the call is cleared.

7.1.6.3 Total & Partial match

A partial match is tested only in case of destination number received in overlap mode. It occurs when the number to be tested is included in the configured prefix. A total match occurs when the configured prefix with the specified length (or upon a timer expiry) is included or equal to the number to be tested.

Example of partial & total match:

Number	Type	Prefix	Length	Match
1000		10	2	No
1000		10**.**	2	Total
1000	Overlap	10**.**	8	Partial
1000	En-Bloc	10**.**	8	No
10	Overlap	1000	4	Partial
10	En-Bloc	1000	4	No
empty	Overlap	all values	> 0	Partial
empty	Overlap	.	0	Total
1000	En-Bloc	.	0	Total

7.1.6.4 Routing Empty Number

Sometimes, it may be necessary to specify a routing rule for an empty number (SETUP message in overlap mode received on an ISDN interface, off-hook event on an analog interface). For that case, a particular syntax is defined: "**-**". The length is equal to 0 and in case of outgoing routing process, the match is considered total (the outgoing routing process is finished).

7.2 VOIP ROUTING CONFIGURATION

7.2.1 Numbering plan description and default type of number

Use the following commands in global voice configuration mode to configure the numbering plan so as OneOS is able to manage the numbering plan (default: `no num-plan-management`).

```
CLI(configure> voice-global
CLI(voice-global)> [no] num-plan-management
CLI(num-plan-mgt)> national-prefix <nn>
CLI(num-plan-mgt)> international-prefix <ii>
CLI(num-plan-mgt)> country-code <CC>
CLI(num-plan-mgt)> exit
CLI(voice-global)> exit
CLI(configure>
```

Use the following command in dial peer voice POTS (FXS) or dial peer voice VoIP (SIP) configuration mode to define the default type of number for FXS and SIP before applying the routing process (default: national calling-number and unknown called-number).

```
CLI(configure)> dial-peer voice pots/voip <n>
CLI(pots/voip)> default-type-of-number { unknown | national }
                                       { calling-number | called-number | all }
```

Notes:

- This command can be entered twice (different calling and called type of number).
- This command is of no effect on dial peer voice POTS (ISDN) and dial peer voice VoIP (H.323).
- The default type of number applied to the calling number is also applied to the number shown in the Redirection IE or the SIP Diversion header.

7.2.2 Pre processing management

The pre-processing allows having a unique format for the numbers (without prefixes and with the ad-hoc type of number according to the numbering plan described in 7.2.1 above) before applying the routing process. Use the following command in dial peer voice POTS (FXS, ISDN) or dial peer voice VoIP (SIP, H.323) configuration mode to apply or not the pre-processing on the calling or/and the called numbers (default: all).

```
CLI(pots/voip)> numplan-preprocessing { none | calling-number
                                      | called-number | all }
```

Notes:

- This command is of no effect (but accepted and saved) if no num-plan-management is in force.
- The pre-processing is also applied to a transferred or rerouted number (if called-number or all apply).
- The pre-processing is also applied to the number shown in the Redirection IE or the SIP Diversion header (if calling-number or all apply).

7.2.3 Dial plan management

To be completed.

7.2.4 Routing table management

The routing table is configurable with the following command.

```
CLI(configure)> voice-routing
CLI(voice-route)>
```

Use the following command to display all the configured routing rules.

```
CLI(voice-route)> display
```

Use the following command to enter in the configuration mode for a routing rule (index from 1 to 200).

```
CLI(voice-route)> route <index>
```

Use the no form to delete the routing rule.

```
CLI(voice-route)> no route <index>
```

Use the following command to insert a routing rule in the list.

```
CLI(voice-route)> insert <index>
```

Example: to enter into the routing rule #1 configuration:

```
CLI(voice-route)> route 1
CLI(conf-voice-route)>
or
CLI(voice-route)> insert 1
CLI(conf-voice-route)>
```

The order of the routing rules in the list is significant: the routing process scans the table from the first to the last rule until a match is found.

7.2.5 Route Configuration

Use the following command to specify, for a wildcard "digit subset", a list of authorized digits. Example: `wildcard C 01234`. Up to eight partial wildcards can be configured. Default: only the letter `X` is configured for `0-9,#,*` (and cannot be modified). This wildcard configuration is specific to the routing rules and is used only for the "prefix" command (NOT for the "translate" command).

```
CLI(conf-voice-route)> wildcard <A-Z a-z> <List of digits 0-9,#,*>
```

Use the no form to remove the wildcard.

```
CLI(conf-voice-route)> no wildcard
```

Use the following command to define a matching prefix with the wildcards method (refer to 7.1.4 and above). The phone digits (0 to 9, #, *****), the wildcards digit subset (when configured), the wildcard any digit ("X"), the wildcard any number ("**.**") and the empty number ("**-**") can be used. The `timer` parameter must be used with certain ISDN phones sending the called number in the Keypad ISDN IE.

```
CLI(conf-voice-route)> prefix <pattern> [to <last-number>]
                       [number-type <type>] [number-presentation <presentation>]
                       [length <0-35>] [timer | timer-or-#] [overlap]
```

- `to <last-number>`: if this optional parameter is present, the number is matched if it is in the range `<pattern>` to `<last-number>`. Therefore, pattern must be a number (i.e. with no wild card).
- `number-type` **{ all | unknown | national | international | network | subscriber | abbreviate }**: specifies the type of number (see ITU-T Q.931) to be checked; all (default value) means "any type of number".

- number-presentation **{ all-presentation | allowed | restricted | number-unavailable}**: specifies the type of presentation of the calling number (see ITU-T Q.931) to be checked; all-presentation (default value) means "any type of calling number presentation".
- length <0-35>: specifies the minimum number of digits to receive before sending the call. Must be greater or equal to the prefix length. Default: equal to prefix length.
- timer: enables the timer mode to complete the dialing phase. It must be disabled if a length is specified. Default: disable.
- timer-or-#: with this parameter, the number is considered complete if the inter-digit timer elapses (same as timer parameter) or if the entered digit is #. The # digit is not considered a dialing digit: if the user calls 30034567#, the called number is 30034567.
- overlap: if enable, the call is sent without the Information Element "Sending Complete", enabling the possibility of overlap dialing. (Significant only for calls coming from an analog local port). Default: disable.

Use the no form to remove the prefix definition.

```
CLI(conf-voice-route)> no prefix
```

Use the following command to define an alternate matching prefix with the wildcards method. It makes it possible to have two matching entries for a single route.

```
CLI(conf-voice-route)> alt-prefix <prefix> [number-type <type>]
                           [length <0-35>] [timer | timer-or-#] [overlap]
```

Use the no form to remove the alternate prefix definition.

```
CLI(conf-voice-route)> no alt-prefix
```

For example, the match of private and public numbering plans (with the wildcards method):

```
route 14
  dial-peer pots-group 4
! match public number
  prefix 0141871004 length 10
! match private number
  alt-prefix 8004 length 4
  prefix-type outgoing called last
! translate private number into public number
  translate ABCD 014187ABCD called
  loopback-routing
 exit
```

Use the following command to define a matching prefix with the regular expressions method. The regular expression is a string up to 255 characters that complies with the syntax described in 7.1.5. Refer to the prefix command above for the explanation of the parameters (the regular expression method allows defining the length of the prefix as well as the alternate prefix within the regular expression string).

```
CLI(conf-voice-route)> regex-prefix <regular-expression>
                [number-type <type>] [number-presentation <presentation>]
                [timer | timer-or-#] [overlap]
```

Use the following command to specify if the prefix must be checked for the incoming routing process or the outgoing routing process or both, and which number must be checked (calling or called).

```
CLI(conf-voice-route)> prefix-type { incoming | outgoing | mixed }
{ called | calling } { last | next | reject | backup } [<bc-type>]
```

For the incoming routing process, the next-route parameter specifies if the routing process must check another rule (next) or not (last) before starting the outgoing routing process or reject the call.

For the outgoing routing process, the next-route parameter specifies if a following backup routing rule must be used in case of outgoing call failure or if the call must be rejected (reject).

The bc-type is the bearer capability type. The call is processed through this route if the bc-type of the received call matches the bearer capability. The bc-type values are:

- full: any bearer capability (default).
- voice: ISDN voice bearer capability.
- data: data bearer capability (ISDN BC= UDI64k or transparent codec –RFC4040-).
- 3k1: ISDN 3.1 kHz bearer capability.
- voice-3k1: voice 3.1 KHz.

Default: outgoing, called, last, and full (any bc type).

Use the no form to remove the prefix type definition.

```
CLI(conf-voice-route)> no prefix-type
```

Use one of the following commands to specify the type of destination.

```
CLI(conf-voice-route)> dial-peer pots-group <identifier>
                                  [ua-sip | alias | gw-prefix] [hunting]

CLI(conf-voice-route)> dial-peer voip <identifier>
        [{ua-sip | ip-address <ip-address> | mac-address <mac-address>}]

CLI(conf-voice-route)> dial-peer voip-group <identifier>

CLI(conf-voice-route)> dial-peer voice-group <identifier>
```

- identifier: local port group if pots-group is selected, dial-peer VoIP index if voip is selected.
- ua-sip (SIP specific): This command allows configuring the various SIP accounts for phone numbers. The registrar address must be defined under the SIP gateway configuration mode. By default, the phone number provided as the route prefix (see prefix command) to this dial-peer is registered. An optional SIP identifier (sip-username) and SIP username & password (sip-authentication) can be specified (see bellow). **WARNING: if several routes must be configured for the same dial-peer, the route containing the** ua-sip **option must be the first one in the voice-routing table**.
- alias | gw-prefix (H.323 specific): the specified prefix or number is used as a H.323/SIP alias or H.323/SIP gateway identifier for registration to a gatekeeper. Optional and authorized only if pots-group is specified.
- hunting: this option enables the hunting mode. Only valid for a pots-group.
- ip-address (syntax: A.B.C.D:<port> or host:<port>): remote IP address (for VoIP type only) if it is not configured in the dial-peer VoIP (without a gatekeeper/SIP proxy).
- mac-address (syntax: aa:bb:cc:dd:ee:ff): remote MAC address (for VoIP type only) if it is not configured in the dial-peer VoIP.

Use the no form to remove the dial-peer.

```
CLI(conf-voice-route)> no dial-peer
```

Use the following command to select a specific external SIP proxy to be used when initiating a SIP outgoing call. via optional parameter defines an outbound proxy (all the SIP signaling messages will be sent to this address).

```
CLI(conf-voice-route)> [no] prox-dns-add { <proxy-ip-address>[:<port>]
                                         | <proxy-name>[:<port>] }
                                         [via <ip-address>[:<port>]]
```

Use the following command to specify the SIP identifier (optional parameter).

```
CLI(conf-voice-route)> [no] sip-username <string 1-120>
```

For a dial-peer pots-group: it is used to specify the SIP identifier used for the "From" & "Contact" header fields of the REGISTER (the `ua-sip` option must be enabled) and INVITE methods. If `sip-username` is empty (default value), the prefix (phone number) is used.

For a dial-peer VoIP: it is used to specify the SIP identifier used for the "To" field. It is used to replace the destination phone number by a name.

Use the `no` form to remove the sip username (default).

```
CLI(conf-voice-route)> no sip-username
```

Use the following optional command to specify the SIP username and password for authentication in the REGISTER and INVITE procedure. For registration authentication the command must be added in the `ua-sip` route while for invite registration the command must be added in a non `ua-sip` route. The optional parameter `type` allows hiding the password in the CLI text file and for a `show running-config` command. `type=0` indicates that the password must be encrypted. `type=1` indicates that the password is already encrypted. If the parameter `type` is absent then the password is unchanged (not encrypted). See an example in 8.1.2.

```
CLI(conf-voice-route)> sip-authentication <username: 1-120 char>
                                          [<password: 1-100 char>] [<type>]
```

Use the `no` form to remove the sip authentication parameters (default).

```
CLI(conf-voice-route)> no sip-authentication
```

Use the following command to force the use of a hostname ("From" and "Contact" header fields) instead of an IP address or default device hostname (configured in the SIP gateway) in REGISTER (the `ua-sip` option must be enabled) and in INVITE. This parameter obsoletes the previous `sip-user` parameter.

```
CLI(conf-voice-route)> sip-device-host-name <host-name: 1-35>
```

Use the `no` form to remove the sip device host name (default).

```
CLI(conf-voice-route)> no sip-device-host-name
```

Use the following command to define authentication (used for SIP server only). See 9.2.3 for more details.

```
CLI(conf-voice-route)> sip-uas-authentication <usrname> <password> <type>
```

Use the `no` form to remove the sip server authentication parameters (default).

```
CLI(conf-voice-route)> no sip-uas-authentication
```

Use the following command to manage the loopback routing

The loopback routing is an attribute to allow an inbound call to be routed to the same origin. By default, a loopback-routing is allowed on a dial-peer pots-group and disabled in case of VoIP dial-peer. The default values correspond to the common case: a call coming from the softswitch (VoIP dial-peer) is not re-routed to the softswitch. A call coming from an ISDN line bundle can be re-routed back to the ISDN (for local calls).

```
CLI(conf-voice-route)> [no] loopback-routing
```

Note: when set, `no loopback-routing` is automatically unset when the call comes from the sip-server entity following a call coming from an external proxy re-routed by the phone to the external proxy.

Use the following command to specify the number of digits to remove at the beginning of the called or calling number (default: called) (optional parameter).

```
CLI(conf-voice-route)> suppress-prefix <prefix 0-35> [calling | called]
```

Use the no form to remove the prefix suppression (default).

```
CLI(conf-voice-route)> no suppress-prefix { calling | called }
```

Use the following command to specify the number to be inserted at the head of the called or calling number (default: called) (optional parameter).

```
CLI(conf-voice-route)> insert-prefix <prefix 0-35> [calling | called]
```

Use the no form to remove the prefix insertion (default).

```
CLI(conf-voice-route)> no insert-prefix { calling | called }
```

Use the following command to specify the number to be inserted at the end of the called or calling number (default: called) (optional parameter).

```
CLI(conf-voice-route)> insert-suffix <suffix 0-35> [calling | called]
```

Use the no form to remove the suffix insertion (default).

```
CLI(conf-voice-route)> no insert-suffix { calling | called }
```

Use the following command to specify advanced translations on the calling or called number.

```
CLI(conf-voice-route)> translate <number-to-translate>
                                 <translated-number> [calling | called]
```

The syntax for the number to translate: "`.`" specifies "any number of any digits", "`0-9`" specifies digits to be compared, "`A-Z`" identifies "any digit".

The syntax for the translated number: "`0-9`" specify fixed digit and "`A-Z`" defines digits specified in the "number to translate".

Example: "`translate .345ABC000 10ABC calling`" specifies a translation of any calling number ending by "345ABC000" to "10ABC" (12345789000 translated to 10789).

Use the no form to remove the translation (default).

```
CLI(conf-voice-route)> no translate { calling | called }
```

Use the following command to replace or insert (if absent) a full calling number information element with a configurable Q.931 CLIP/CLIR header.

```
CLI(conf-voice-route)> insert-calling <number 0-35> [type <type value>]
[plan <num plan>] [presentation <value>] [screening <value>]
```

- `type`: 0=unknown, 1=international, 2=national, 3=network, 4=subscriber, 6=abbreviated.
- `plan`: 0=unknown, 1=isdn, 3=data, 4=telex, 8=national, 9=private.
- `presentation`: 0=allowed, 1=restricted, 2=unavailable.
- `screening`: 0=not-screened, 1=verified-passed, 2=verified-failed, 3=Network

Default: type=0, plan=0, presentation=0, screening=0.

Example: `insert-calling 456 type 3 plan 1 presentation 0 screening 1`

Use the no form to remove the calling number insertion (default).

```
CLI(conf-voice-route)> no insert-calling
```

Use the following command to force the calling number header for the Calling Line Identification Restriction complementary service. See 4.2.3.2 for permitted values.

```
CLI(conf-voice-route)> force-clir <presentation code> <screening code>
```

Use the no form to remove the CLIR configuration (default).

```
CLI(conf-voice-route)> no force-clir
```

Use the following command to force the type of numbering plan for the called or the calling number. See ITU-T Q.931 for the values. Example: `force-numplan 17 called` and `ins-prefix 1` adds the international prefix for USA (+1). This function is protocol independent.

```
CLI(conf-voice-route)> force-numplan <numplan 0-127> { called | calling }
```

Use the no form to remove the type of numbering plan configuration (default).

```
CLI(conf-voice-route)> no force-numplan
```

Use the following command to force the Bearer Capability Information Element to the desired value. (Note: µ law – written u law – is used in the USA and Japan). If the destination number is an ISDN data terminal (video, fax group 4), you must select `unrestricted` here and force the voice codec to be G.711A.

```
CLI(conf-voice-route)> force-bearer-cap { speech-a | speech-u
                                        | unrestricted | audio-a | audio-u }
```

Use the no form to remove the Bearer Capability configuration (default).

```
CLI(conf-voice-route)> no force-bearer-cap
```

Use the following command to specify the emergency level of the call. The emergency level is updated only if it is lower than the current value, which is assigned to the call. It can be used for the incoming or the outgoing routing process.

```
CLI(conf-voice-route)> emergency <1..200>
```

Use the no form to set the emergency level to 100 (default).

```
CLI(conf-voice-route)> no emergency
```

Use the following command to provide a service of device reboot, optionally with a new configuration file, for maintenance purpose. This service is enabled only for the incoming routing process. The file name can be present in any directory of the file system. It replaces the current configuration file defined in `bsaBoot.inf`. The old configuration file is lost. This functionality enables to reboot the router with a default configuration file.

```
CLI(conf-voice-route)> startup-file <file name>
```

7.2.6 Call distribution

Once the routing process matches a route, the calls are distributed over the ports according to the priority indicated in the dial-peer POTS, the POTS group, the dial-peer VoIP, the VoIP group or the voice group (refer to the corresponding `priority` commands and to 5.1.2).

Use the following commands in global voice configuration mode to define how calls are distributed within a group among ports (dial peers) with the same priority (default: round robin).

```
CLI(configure> voice-global
CLI(voice-global)> call-distribution { round-robin | load-balancing }
CLI(voice-global)> exit
CLI(configure>
```

7.2.7 Post processing management

The post-processing allows defining the format of the numbers after having applied the routing process.

Use the following command in dial peer voice POTS (FXS, ISDN) or dial peer voice VoIP (SIP, H.323) configuration mode to define the format of the international numbers (default: supported all).

```
CLI(pots/voip)> international-numplan {not-supported |supported | forced}
                                      { calling-number | called-number | all }
```

With `supported`: an international number is sent in ISDN with the type of number international and in SIP with the prefix +.

With `not supported` an international number is sent with the international prefix (see num-plan-management) and the type of number unknown. This is the preferred value especially for FXS.

With `forced` all numbers, including national numbers, are sent as international numbers.

Notes:

- This command can be entered twice (different management for calling and called numbers).
- This command is of no effect (but accepted and saved) if no num-plan-management is in force.
- This command also applies to a transferred or rerouted number (if called-number or all apply).
- This command also applies to the number shown in the Redirection IE or the SIP Diversion header (if calling-number or all apply).

Use the following command in dial peer voice POTS (FXS, ISDN) or dial peer voice VoIP (SIP, H.323) configuration mode to define the format of the national numbers (default: supported all).

```
CLI(pots/voip)> national-numplan { not-supported | supported }
                                 { calling-number | called-number | all }
```

With `supported` no specific process is done.

With `not supported` a national number is sent with the national prefix (see num-plan-management) and the type of number unknown. This is the preferred value especially for FXS and SIP.

Notes:

- This command is of no effect (but accepted and saved) if no num-plan-management is in force.
- This command also applies to a transferred or rerouted number (if called-number or all apply).
- This command also applies to the number shown in the Redirection IE or the SIP Diversion header (if calling-number or all apply).

7.3 USE OF THE ROUTING TABLE FOR SIP NAMING

The routing table may be used to configure specific SIP username or hostname for a voice port or each subscriber. If necessary, routing rules may be defined only for that purpose.

7.3.1 Registration

The OneOS-based voice-capable router checks every routing rule including the `ua-sip` option and concerning a local pots-group. For each rule, a REGISTER message is sent with the prefix (optionally replaced by the sip-username parameter), the default hostname (optionally replaced by the sip-device-host-name parameter).

7.3.2 Call Signaling

Call Signaling: Outgoing Call

For each new call, the OneOS-based voice-capable router checks in the whole routing table if the calling number matches with the prefix number of a rule “outgoing routing and called number” or “incoming routing and calling number” concerning the local port where the call comes from. If a match occurs, the "From" and "Contact" header fields will be built from the optional parameters sip-username and sip-device-host-name instead of the calling number and default hostname. Authentication parameters, if configured, may also be used.

The default value of the "To" field is the called phone number. It can be replaced by a name if the rule used for the outgoing routing on dial-peer VoIP includes a sip-username parameter.

Call Signaling: Incoming Call

If the "To" field is a username (not a phone number), the relevant routing rules (outgoing type, concerning local ports only) are checked to find a match with a sip-username. If it is found, the called phone number is determined by the prefix.

For each provisional response, the "From" header field and the "To" header field are identical respectively to the "From" header field and the "To" header field received in the INVITE message. For the 200OK message, the "Contact" header field is updated the same way as for the "From" header field of the outgoing call (the routing table is checked to find the called number).

Example: defining and registering a sip-username user_1 for subscriber 3001. The subscriber is registered and identified as “user_1”.

```
Route 4
 prefix 3001
 dial-peer pots-group 1 ua-sip
 prefix-type outgoing called
 sip-username user_1
exit
```

Example: defining a hostname “name1” specific for a voice-port (pots 2) with a dedicated routing rule.

```
Route 4
 prefix .
 dial-peer pots 2
 prefix-type incoming calling
 sip-device-host-name name1
exit
```

7.4 CALL BACKUP ROUTING PARAMETERS

7.4.1 Backup Criteria: Q.850 Release Causes

A call can be routed via a backup route in case of connection failure when the backup option is selected. The failure causes (defined in ITU-T Q.850) allowing a call backup to be processed are configurable. Up to 8 classes of causes are defined in the standard. Each class includes several cause values among 16 possible, that means 128 causes at maximum.

```
CLI(configure)> voice-routing
CLI(voice-route)> backup-cause
CLI(backup-cause)> add { class | value } <value>
CLI(backup-cause)> remove { class | value } <value>
CLI(backup-cause)> exit
```

By default, all causes belonging to Class 0 and 1 disallow call backup routing and all causes belonging to Class 2 to 7 allow call backup routing.

To add (call backup allowed) or remove (call backup forbidden) a full class use `add/remove class <0..7>`. To add or remove a specific cause use `add/remove value <0..127>`.

Use the no form to re-apply the default call backup configuration.

```
CLI(voice-route)> no backup-cause
```

Note: the configuration is taken into account by the “exit” command.

Use the following command to display the current call backup configuration (list of causes).

```
CLI(backup-cause)> display
```

7.4.2 Backup Timers

A global timer can be configured for backup. It is used when the timeouts on the outbound call-leg are too long: it becomes necessary to start the backup process before the timeout on the inbound call-leg expires.

```
CLI(configure)> voice-routing
CLI(voice-route)> backup-timer <duration 5..60sec>
CLI(voice-route)> exit
```

Default: 10 seconds.

Note: this timer only applies in case of SIP outbound call.

8 VOIP EXAMPLES, STATISTICS AND DEBUG

8.1 VOIP CONFIGURATION EXAMPLES

- Rule 1: any number using this format '30xxxx' is routed to the dial-peer voip #1 (IP address 172.30.40.2), the first four digits are suppressed.
- Rule 2: the destination number starting by 4001 is routed to the local port group #1 and is used as a H.323/SIP alias for registration.

```
voice-routing
  route 1
    prefix 30 length 4 overlap
    dial-peer voip 1 gw-addr 172.30.40.2
    supp-prefix 4
    exit

  route 2
    prefix 4001 length 4
    dial-peer pots-group 1 alias
    supp-prefix 4
    exit
```

To display the routes:

```
CLI(voice-route)> display
1 – 30 length 4 voip 2 [172.30.40.2] supp 4
2 – 4001 length 4 pots 1 alias supp 4
CLI(voice-route)>
```

It is possible to test the routing table with the following command:

```
CLI(voice-route)> test <called number> <calling number>
                                    {from-pots | from-voip} <dial-peer id>
```

8.1.1 Configuration Example

To use these configuration examples, copy & paste the following command lists in a configuration file or to the CLI.

Configuration environment: 4 BRI ports, use of a gatekeeper, registration if a minimum of 4 digits prefix for admission request, coder G.729AB and G.711, no fast connect.

```
! Physical voice ports declaration
voice-port 5/0
exit
voice-port 5/1
exit
voice-port 5/2
exit
voice-port 5/3
exit
```

```
! BRI interface parameters
interface bri 5/0
isdn
application-interface voip
protocol-emulation isdn-nt
exit
exit

interface bri 5/1
isdn
application-interface voip
protocol-emulation isdn-nt
exit
exit

interface bri 5/2
isdn
application-interface voip
protocol-emulation isdn-nt
exit
exit

interface bri 5/3
isdn
application-interface voip
protocol-emulation isdn-nt
exit
exit

! local voice ports

dial-peer voice pots 0
pots-group 1
port 5/0
exit
dial-peer voice pots 1
pots-group 1
port 5/1
exit
dial-peer voice pots 2
pots-group 1
port 5/2
exit
dial-peer voice pots 3
pots-group 1
port 5/3
exit

! H323 gateway global parameters (gatekeeper)

h323-gateway
gw-interface fastethernet 0
gatekeeper id ZONE1 ipaddr 10.2.2.1
h323-id GW1
no shutdown
exit

! Voice coder list (terminal capabilities)

voip-coder-profile 1
codec 1 g729ab 20
codec 2 g711a 20
exit

! dial-peer voip: remote voip devices

dial-peer voice voip 1
```

```
gatekeeper mandatory
no fast-connect
voip-coder-profile 1
silence-detection vad
implicit-routing pots-group 1
exit

! routing table

voice-routing
route 1
prefix . length 4
dial-peer voip 1
exit
exit
```

8.1.2 Authentication example

Route 1 is used for invite authentication and route 102 for registration authentication.

```
Voice-routing
 route 1
  dial-peer pots-group 0
  sip-authentication +33320030001@antwerp.ft.com test
  prefix-type incoming calling next
  prefix . timer-or-#
  no loopback-routing
 exit
 route 91
  dial-peer voip 0
  prefix-type outgoing called last
  prefix . timer-or-#
  no loopback-routing
 exit
 route 102
  dial-peer pots-group 0 ua-sip hunting
  sip-authentication +33320030001@antwerp.ft.com test
  prefix-type outgoing called last
  prefix 31356876052 length 11
  suppress-prefix 2 called
  force-numplan 33 called
  no loopback-routing
 exit
exit
```

8.1.3 Backup example

Route 2 on ISDN is used as backup when route 1 VoIP is no more available.

```
Interface bri 5/0
 isdn
  protocol-emulation isdn-nt
 exit
 no shutdown
 execute
exit
voice-port 5/0
 clock-source free_run
exit
dial-peer voice pots 0
 pots-group 0
 port 5/0
```

```
 no shutdown
exit
dial-peer voice voip 0
 sig-protocol sip
 gw-ip-address 192.168.1.2
 voip-coder-profile 0
 no shutdown
exit
voice-routing
 route 1
  dial-peer voip 0
  prefix-type outgoing called backup
  prefix .   timer-or-#
  no loopback-routing
 exit
 route 2
  dial-peer pots-group 0
  prefix-type outgoing called last
  prefix .   timer-or-#
  loopback-routing
 exit
exit
sip-gateway
 no calling-number-checking
 gw-interface fastethernet 0 intrusive
 no shutdown
exit
voip-coder-profile 0
 codec 0 g711a 20
exit
```

8.2 VOIP STATISTICS

The Command Line Interface provides access to statistics and configuration status for the voice service. The show commands can be used at any level in the CLI tree.

The syntax is the following:

```
CLI> show voice <function> [<parameter> [{ index <index> | all }]]
```

function defines the voice function

parameter defines the type of port or connection within the function

index specifies the port or connection number within the type; all specifies all ports or connections.

8.2.1 Running Configuration

The following command provides the current voice configuration with a list of CLI commands that are the exact differences between the current configuration and the default configuration. This command enables easy replication of configuration over other devices.

This set of commands can be entered in another device to set up the voice service with the same parameters. First, it is preferable to use the voice-default CLI command to ensure that the device starts with the same default configuration.

```
CLI> show voice running-config
Building configuration…
voice-default
voice-port 5/0
 clock-source free_run
 echo-disable modem
 metering  0
 aoc-d-service forced
 aoc-e-service forced
 no led-alarm-report
exit
voice-port 5/1
 clock-source free_run
 echo-disable modem
 metering  0
 aoc-d-service forced
 aoc-e-service forced
 no led-alarm-report
exit
dial-peer voice pots 0
 pots-group 0
 port 5/0
 no shutdown
exit
dial-peer voice pots 1
 pots-group 0
 port 5/1
 no shutdown
exit
dial-peer voice voip 0
 call-media-independant
 dtmf-relay in-band
 fax-relay t38orpassthrough priority t38
 gatekeeper mandatory
 h245-tunnel
 modem-passthrough
```

```
 passthrough-mode request-mode
 voip-coder-profile 0
 aoc-format ecma aoc-e-generation remote
 no shutdown
exit
voice-routing
 route 1
  dial-peer pots-group 0
  prefix-type incoming called last
  prefix .  length 0
  insert-prefix #99 called
  loopback-routing
 exit
 route 2
  dial-peer voip 0
  prefix-type outgoing called last
  prefix #993651.  length 8  overlap
  suppress-prefix 7 called
  force-clir  1 1
  no loopback-routing
 exit
 route 3
  dial-peer voip 0
  prefix-type outgoing called last
  prefix #99.  length 4  overlap
  suppress-prefix 3 called
  force-numplan  0 called
  no loopback-routing
 exit
 route 4
  dial-peer voip 0
  prefix-type incoming calling last
  prefix .  length 0
  insert-prefix #98 calling
  no loopback-routing
 exit
 route 5
  dial-peer pots-group 0 hunting
  prefix-type outgoing calling last
  prefix #98.  length 3
  suppress-prefix 3 calling
  loopback-routing
 exit
exit
h323-gateway
 gw-address autoconfig
 gw-interface bvi 1
 q931-connection-timeout 180
 bandwidth-control  ratio 100 rate current-rate
 gw-interface-bw-ctrl
 set-portability enable timeout 4320
 payload-64k-unrestricted 101
 no shutdown
exit
sip-gateway
 shutdown
exit
sip-server
 shutdown
exit
voip-coder-profile 0
 codec 0 g729ab 20
 codec 1 g711a 20
exit
CLI>
```

8.2.2 Voice Hardware and Software versions

To show the voice hardware configuration, enter:

```
CLI> show voice hardware full
Voice module : 6 lines
MotherBoard  : 2 BRI
Ext Module   : MF100
             : 4 FXS
```

To show the voice software version, enter:

```
CLI> show voice version
Voice VOIP  version: _V29B (28/05/09 19:47:53)
Voice DSP   version:    40536
```

8.2.3 Voice global information and memory

To show the global voice information, enter:

```
CLI> show voice global information
no hardware limitation (8 max) voice com.
Maximum of SIP simultaneous calls       : 8
maximum of SIP registration endpoints   : 15
```

To show the global voice memory information, enter:

```
CLI> show voice global memory
maximum size of SIP message  : 8192 byte(s)
```

8.2.4 ISDN active calls

To display the list of active (connected) calls using ISDN ports, enter:

```
CLI> show isdn active
------------------------------------------------------------------------------
                       ISDN ACTIVE CALLS
------------------------------------------------------------------------------
App.  Call     Calling       Called   Call   Port BChan Call-ref call-id
      Type      Number       Number Duration
------------------------------------------------------------------------------
 Data Out               2123456789 00:09:05  5/2   1        6       21
 Data Out               2123456789 00:08:59  5/2   2        7       23
 Data Out               2123456789 00:08:59  5/3   1        4       22
Voice  In         1001         1006 00:00:49  5/4   1        3       13
Voice Out         1005         1004 00:00:06  5/5   1        2       18
------------------------------------------------------------------------------
```

8.2.5 BRI/S0 Voice Port Statistics

The command to display statistics on a BRI voice port is (in this example, voice port number 0):

```
CLI> show voice voice-port bri index 0
        voice port                          5/0
                protocol descriptor         BRI_NT
                config state                down
                layer 1 status              deactivated
                layer 2 status              TEI , status
```

```
attached voip dial peer         0
number of voice communication   0
Channel(s) used

bri Tx frames on D channel      0
bri Rx frames on D channel      0

Outgoing calls                          0
Outgoing calls failures                 0
        Unsufficient pots-group resource        0
        Physical Interface down                 0
        Cause Class 0 (normal event)            0
        Cause Class 1 (normal event)            0
                Normal Cause (16)               0
                User busy (17)                  0
                No answer (18)                  0
        Cause Class 2 (unavailable resources)   0
        Cause Class 3 (unavailable service)     0
        Cause Class 4 (service not provided)    0
        Cause Class 5 (invalid message)         0
        Cause Class 6 (protocol error)          0
        Cause Class 7 (interworking)            0

Incoming calls                          0
Incoming calls backup invoked           0
Incoming calls failures                 0
        Remote failure                          0
        Unknown number                          0
        DSP unavailable                         0
        No VoIP ressource available             0
        Not specified                           0
```

Notes:

- Outgoing call statistics are related to the calls towards the ISDN device or network (transmitted by the OneOS-based voice-capable router on this port).
- Incoming call statistics are related to the calls coming from the ISDN device or network (received by the OneOS-based voice-capable router on this port). "Remote failure" indicates that the failure has occurred on the outbound port (VoIP or local).
- The layer 1 state (layer 1 status) may be deactivated if no communication is in progress.
- Number of voice communications: 0, 1 or 2. Current number of communications in progress.
- `show voice voice-port bri all` displays statistics on all the voice ports

8.2.6 PRI Voice Port Statistics

The following command returns statistics about the physical E1/PRI port.

```
CLI> show voice voice-port pri index 0
  voice port                        5/0
    physical type                   E1
    protocol descriptor             E1_PRI
    config state                    up
    framing                         EMF
    layer 1 status                  activated
    layer 2 status                  TEI , status
                                      0 , established

    attached voip dial peer         0
    number of voice communication   0
    pri AIS occurrence              0
    pri RDI occurence               0

    Outgoing calls                              11358
    Outgoing calls failures                     278
      Unsufficient pots-group resource          0
```

```
    Physical Interface down                0
    Cause Class 0 (normal event)           0
    Cause Class 1 (normal event)           277
      Normal Cause (16)                    0
      User busy (17)                       76
      No answer (18)                       0
    Cause Class 2 (unavailable resources)  0
    Cause Class 3 (unavailable service)    0
    Cause Class 4 (service not provided)   0
    Cause Class 5 (invalid message)        1
    Cause Class 6 (protocol error)         0
    Cause Class 7 (interworking)           0

  Incoming calls                           16408
  Incoming calls backup invoked            0
  Incoming calls failures                  1411
    Remote failure                         1411
    Unknown number                         0
    DSP unavailable                        0
    No VoIP ressource available            0
    Not specified                          0
```

Note:

- Outgoing call statistics are related to the calls towards the ISDN device or network (transmitted by the OneOS-based voice-capable router on this port)
- Incoming call statistics are related to the calls coming from the ISDN device or network (received by the OneOS-based voice-capable router 0 on this port). "Remote failure" indicates that the failure has occurred on the outbound port (VoIP or local).
- The "number of voice communications" is the number of communications in progress.
- `show voice voice-port pri all` displays statistics on all the voice ports.

8.2.7 FXS Voice Port Statistics

To show statistics on a FXS physical port, enter:

```
CLI> show voice voice-port fxs index 0
       voice port                              5/2
              current state                    off hook
              config state                     up
              attached voip dial peer          6
              voice communication              1

              Outgoing calls                          0
              Outgoing calls failures                 0
                     Unsufficient pots-group resource        0
                            User busy (17)                   0
                            No answer (18)                   0

              Incoming calls                          5
              Incoming calls backup invoked           0
              Incoming calls failures                 1
                     Remote failure                          1
                     Unknown number                          0
                     DSP unavailable                         0
                     No VoIP ressource available             0
                     Not specified                           0
```

Note:

- Outgoing call statistics are related to the calls towards the FXS device or network (transmitted by the OneOS-based voice-capable router on this port).
- Incoming call statistics are related to the calls coming from the FXS device or network (received by the OneOS-based voice-capable router on this port). "Remote failure" indicates that the failure has occurred on the outbound port (VoIP or local).

- Voice communication indicates the number of communications in progress (usually 0 or 1).

To show statistics on all FXS physical ports, enter:

```
CLI> show voice voice-port fxs all
```

8.2.8 FXO Voice Port Statistics

To show statistics on a FXO physical port, enter:

```
CLI> show voice voice-port fxo index 12
        voice port                              5/12
                current state                   on hook
                config state                    up
                attached voip dial peer         0
                voice communication             no
                Line voltage                    0 V
                Loop current                    0.000000 mA

                Outgoing calls                          0
                Outgoing calls failures                 0
                        Insufficient pots-group resource        0
                                User busy (17)                  0
                                No answer (18)                  0

                Incoming calls                          0
                Incoming calls backup invoked           0
                Incoming calls failures                 0
                        Remote failure                          0
                        Unknown number                          0
                        DSP unavailable                         0
                        No VoIP resource available              0
                        Not specified                           0
```

Note:

- Outgoing call statistics are related to the calls towards the FXO device or network (transmitted by the OneOS-based voice-capable router on this port).
- Incoming call statistics are related to the calls coming from the FXO device or network (received by the OneOS-based voice-capable router on this port). "Remote failure" indicates that the failure has occurred on the outbound port (VoIP or local).
- Voice communication indicates yes or no according to communication in progress or not.

To show statistics on all FXO physical ports, enter:

```
CLI> show voice voice-port fxo all
```

8.2.9 Dial Peer VoIP Statistics

To show statistics for the dial-peer VoIP <port-id>, use the following command:

```
CLI> show voice dial-peer voice voip index <port-id> [<type>] [reset]
```

To show statistics for all the dial-peer VoIP, use the following command:

```
CLI> show voice dial-peer voice voip all [<type>] [reset]
```

type may be:

- current: statistics on current calls.
- outgoing: statistics on outgoing calls only.
- incoming: statistics on incoming calls only.
- user-plan: statistics on voice & fax only.
- all (default): all the statistics are provided.

```
CLI> show voice dial-peer voice voip index 0
Dial Peer                                                1
 Current protocol                        h323
 Current Calls                                           1
                        Outgoing Calls
         Outgoing Calls                  221
         Outgoing calls failures         14
         RAS Call Failures                       0
                 Admission time-out                      0
                 Admission Rejects                       0
         H225/Q931 Call failures                 14
                 Cause Class 0 (normal event)            0
                 Cause Class 1 (normal event)            4
                         Normal Cause (16)               0
                         User busy (17)                  0
                         No answer (18)                  0
                 Cause Class 2 (unavailable ressources)  10
                 Cause Class 3 (unavailable service)     0
                 Cause Class 4 (service not provided)    0
                 Cause Class 5 (invalid message)         0
                 Cause Class 6 (protocol error)          0
                 Cause Class 7 (interworking)            0
                H245 Call failures                      0
                 Incompatible capabilities               0
                 Protocol errors                         0
         Internal call failures                  0
                 DSP unavailable                         0
                 Max-bandwidth exceeded                  0
                 Max-connection exceeded                 0
                 Gateway not registered                  0
                 Gateway status down                     0
                 Not specified                           0
                         Incoming Calls
         Incoming calls                  345
         Incoming calls failures         14
         RAS Call failures                       0
                 Gatekeeper Unavailable                  0
                 Admission Rejects                       0
         Local Port Call failures                0
         H245 Call failures                      0
                 Incompatible capabilities               0
                 Protocol errors                         0
         Internal call failures                  14
                 DSP unavailable                         0
                 Unknown number                          0
                 Channel / port unavailable              0
                 Max-bandwidth exceeded                  0
                 Max-connection exceeded                 0
                 Not specified                           14
         Advice-of-charge                        0
                         Voice & Fax statistics
 RTP statistics
         Number of transmitted packets                   35
         Number of received packets                      40
         Number of transmitted bytes                     11620
         Number of received bytes                        13280
         Number of excessive jitter events               0
         Number of lost packets                          0
         Number of invalid packets                       0
 Number of calls with frame error rate
          total <0.01%  <0.1%  <0.5%    <1%    <5%   >=5%
            565    565      0      0      0      0      0
 Modem passthrough
         Number of switching to modem mode               0
 T38 FAX Calls
         Number of outgoing fax                          0
         Number of incoming fax                          0
```

```
Number of failures                          0
        Request Mode failure                0
        Pre-message procedure failure       0
        Page failure                        0
Number of transmitted packets               0
Number of received packets                  0
Number of transmitted bytes                 0
Number of received bytes                    0
Number of lost packets                      0
```

Note:

- Outgoing call statistics are related to the calls towards the H.323/SIP network (transmitted by the OneOS-based voice-capable router to the remote VoIP device.
- Incoming call statistics are related to the calls coming from the H.323/SIP network (received by the OneOS-based voice-capable router from a VoIP device). "Remote failure" indicates that the failure has occurred on the outbound port (local).

8.2.10 MOS Scoring Statistics

The following command gives statistics about the voice quality:

```
CLI> show voice mos

------------------------- Call Quality -------------------------

    Number of Call       : 10
    Average of MOS       : 3.58
    Minimum MOS          : 2.38
    Maximum MOS          : 4.29
    Average of ERL       : 41
    Average of ACOM      : 67
    Average of loss-rate : 0
    Average of jitter    : 14
    Average of Max delay : 16
----------------------------------------------------------------
```

Use the following command to reset and restart the MOS scoring statistics:

```
CLI> show voice mos reset
```

8.2.11 H.323 Gateway Statistics

The following command gives statistics about the gatekeeper:

```
CLI> show voice h323-gateway

  H323-Gateway statistics :
  State                                 UP
  Bandwidth used/unused           174800 / 2897200 bps
  Max Bandwidth exceeded                0
  H323 resource threshold is Disable and NOT Active
  Registration state                    unregistered
  Gatekeeper Identifier
  Gatekeeper Address                    0.0.0.0
  Registration requests                 0
  Registration failures                 0
          No response                   0
          Invalid IP address            0
          Duplicate alias               0
          Invalid terminal type         0
          Ressource unavailable         0
          Invalid alias                 0
          Security denial               0
          Undefined reason              0
```

```
Admission requests                      0
Admission rejects                       0
        Called party not registered     0
        Invalid permission              0
        Request denied                  0
        Caller not registered           0
        Resource unavailable            0
        Security denial                 0
        Invalid Endpoint Ident.         0
        Incomplete address              0
        Not specified                   0
        Undefined reason                0
```

8.2.12 SIP Gateway Statistics

The following command gives statistics about the SIP proxy:

```
CLI> show voice sip-gateway
   Gateway state                    up
   Registration state          registered
   Registrar server            100.12.0.2:5060
   Registration errors         0
   Registration requests       2

   Current calls               0

   Authentication Rejects      0
```

8.2.13 Events

- `Layer 1 on ISDN BRI port <5/x> <activated or deactivated>`: ISDN layer 1 state (info).
- `Layer 1 Error on ISDN BRI port <5/x> : <activation failure / deactivation>`: ISDN layer 1 error. Can indicate that the ISDN line is disconnected.
- `Layer 1 on E1/T1 port <5/x> <activated or deactivated>`: G703/G704 state on PRI port.
- `Alarm on E1/T1 port <5/x>: <LOS, AI, RAI, End of LOS, End of AI, End of RAI>`: Alarm detected on PRI port (compliant to G704).
- `FXS port <off-hook>, <on-hook>, <ringing on>, <ringing off>`: Event on FXS analog port.
- `Voice port <5/x> status change <shutdown / no shutdown>`: Indicates that the interface has been shutdown by the operator. The port cannot be used for calls.
- `H323 Gateway registered with the Gatekeeper <gk id>`: gateway registered.
- `H323 gateway registration failure cause <cause>`: registration failure.
- `Incoming call on <voip | local> port <n° port>, calling <E164 number>, called <E164 number>, call-id=<internal call identifier>`: incoming call.
- `Outgoing call on <voip | local> port <n° port>, number <E164 number>, call-id=<internal call id>`: outgoing call on a local or VoIP port.
- `Incoming call failure on <voip | local> port <n° port>, call-id=<internal call id>, cause: <cause>`. Occurs when the call cannot be routed (wrong number, no resource).
- `Outgoing call failure on <voip | local> port <n° port>, call-id=<internal call id>, cause: <Q850 cause> or <RAS cause>`. Occurs if a routed call is released before having reached the “ALERTING” state.
- Overlap dialing, call-id=<internal call id>, number: <digits>: sent for each digit received in overlap dialing mode.

- `Alert received, call-id=<internal call id>`: the call has entered in “alerting” state.
- `Call connected, call-id=<internal call id>`: the call is connected (signaling only). It does not mean that the voice path is established.
- `VoIP RTP transmission <started | stopped>, call-id=<internal call id>, coder <coder>`: indicates that the OneOS-based voice-capable router has started (or stopped) to send RTP packets.
- `VoIP RTP reception <started | stopped>, call-id=<internal call id>, coder <coder>`: indicates that the OneOS-based voice-capable router is able (or not able) to receive RTP packets.
- `VoIP media channel opening failure, call-id=<internal call id>, cause: <H245 cause>`: occurs if the media channel negotiation has failed.
- `Call disconnection received on <voip | local> port <n°port>,, call-id=<internal call id>, cause : < Q850 cause>`: indicates that a disconnection has been received.
- `Local call disconnection, call-id=<internal call id>, cause: <internal cause>`: disconnection sent by the OneOS-based voice-capable router upon an error (DSP down, media channel closed…).
- `H245 <alpha | signal> <DTMF <number> | Hookflash> <sent | received>, callid=<internal call id>`: occurs for each DTMF digit sent or received on the H.323 part of the call.
- `FAX T38 starting, call-id=<internal call id>`: start of the T38 call.
- `FAX T38 end of call, call-id=<internal call id>`: end of the T38 call.
- `FAX T38 call failure, call-id=<internal call id>, cause`: <T38 cause>: indicates the cause of the T38 call failure.
- `FAX T38 Pre-message procedure OK ,call-id=<internal call id>`: indicates that the T38 call is connected.
- `FAX T38 <receiving | transmitting> page <n>, call-id=<internal call id>`: indicates that the page n is being received / transmitted.
- `FAX T38 page <n> <OK | KO>, call-id=<internal call id>`: indicates that the page n has been received / transmitted OK or not.
- `FAX T38 <n> IFP packets lost, call-id=<internal call id>`: indicates a T38 transmission error.
- `FAX/Modem start of detection, call-id=<internal call id>`: indicates that a fax or modem call is being detected.
- `FAX/Modem end of detection, call-id=<internal call id>`: indicates that the detection phase has ended.
- `DSP failure <dsp number>: <cause of failure>`: indicates a DSP internal error (software crash).
- `<number> invalid voice packets received, call-id=<internal call id>`: number of invalid voice packets received.
- `<number> voice packets lost, call-id=<internal call id>`: number of voice packets lost.
- `<number> excessive jitter, call-id=<internal call id>`: the jitter is greater than the configured value.
- `Reboot on voice call reception, call-id=<internal call id>`: remote reboot command has occurred.
- `Portability status: <done | in-progress | disable | enable>`: indicates a change of the number portability state.

Notes:

- <n°port> includes the B channel if the port type is BRI or PRI, except if it is not known (in TE emulation mode, for example).
- <internal call id> is a unique identifier for the call.
- <Q850 cause>: Refer to ITU-T Q.850 cause.
- <H245 cause>: May be "capabilities mismatch", "no remote opening channel", "H.245 protocol error".

8.3 VOIP TROUBLESHOOTING TOOLS

Events and statistics described above should be used first for troubleshooting call failure. This section describes other useful tools.

8.3.1 LEDs

On the front panel, one LED (2 LEDs on ONE200/400) indicates the status of the voice service.

The voice service is fully operational if all these conditions are OK:

- The IP interface attached to the H.323/SIP gateway is UP.
- The H.323/SIP gateway is registered with a gatekeeper or registrar (if configured).
- All the voice interfaces which are in `no shutdown` state are UP. Note that it is possible to exclude a certain voice interface from this condition using the `no led-alarm-report` command under voice-port configuration.

8.3.1.1 ONE200/400 (two "Voice" LEDs)

Led **`Voice`**:

- Green: Voice service fully operational.
- Blinking green: Voice service fully operational. No succeeded call yet.
- Red: Voice service configured but not fully operational (see 8.3.1 above).
- Off: The voice service is not configured.

Led **`Com`**:

- Green: At least one voice call is in progress.
- Off: No voice call is in progress.

8.3.1.2 Other ONEXX0 devices (only one "Voice" LED)

Led **`Com`**:

- Green: Voice service fully operational.
- Blinking green: Voice service fully operational. Call in progress.
- Blinking orange: Voice service fully operational. No succeeded call yet.
- Red: Voice service configured but not fully operational (see 8.3.1 above).
- Off: The voice service is not configured.

8.3.2 ISDN Signaling Capture

It is possible to display all the ISDN protocol messages exchanged between the OneOS-based voice-capable router and the ISDN terminal. Such traces rely on the generic `logging` function (cf. IP debugging in OneOS Book).

Enter the following command:

```
CLI> [no] debug isdn { 5/<0..7> | 2/0 | all } [layer { 1 | 2 | 3 | 1&2
                                                | 2&3 | 1to3} [full] ]
```

The first command argument is the ISDN port(s), whose ISDN messages will be logged. The second argument `layer` is the monitored ISDN layers (1: physical, 2: LAPD, 3: call control and other ISDN applicative messages). The last optional argument `full` allows layer 3 information elements (IE) being decoded.

Example (ISDN Capture from a Telnet Session)

```
CLI> configure terminal
CLI> logging buffered debug
CLI> debug isdn all layer 1to3
CLI> monitor trace
```

Unnumbered frame with a SETUP sent to an ISDN phone

```
00:07:21.271 line:5/0 L1 frame sent.
00:07:21.271 line:5/0 L2 tx UI P/F=0 NR=4 NS=2 C/R=1.
00:07:21.271             hex: 02 ff 03
00:07:21.271 line:5/0 L3 tx SETUP callref:8.
00:07:21.271              hex1: 08 01 08 05 04 03 80 90 a3 18 01 89 70 05
a1 33
00:07:21.272             hex2: 30 33 36 a1
```

Layer 2 establishment

```
00:07:21.343 line:5/0 L1 frame received.
00:07:21.343 line:5/0 L2 rx SABME P/F=1 C/R=0.
00:07:21.343             hex: 00 01 7f
00:07:21.343 line:5/0 L1 frame sent.
00:07:21.343 line:5/0 L2 tx UA P/F=1 NR=4 NS=2 C/R=0.
00:07:21.343             hex: 00 01 73
```

The ISDN phone takes the call

```
00:07:21.380 line:5/0 L1 frame received.
00:07:21.381 line:5/0 L2 rx I P/F=0 NR=0 NS=0 C/R=0.
00:07:21.381             hex: 00 01 00 00
00:07:21.381 line:5/0 L3 rx CALL PROCEEDING callref:8.
00:07:21.381             hex1: 08 01 88 02 18 01 89
00:07:21.381 line:5/0 L1 frame sent.
00:07:21.382 line:5/0 L2 tx RR P/F=0 NR=1 NS=2 C/R=0.
00:07:21.382             hex: 00 01 01 02
```

The ISDN phone indicates that the user is alerted (ringing)

```
00:07:21.412 line:5/0 L1 frame received.
00:07:21.413 line:5/0 L2 rx I P/F=0 NR=0 NS=1 C/R=0.
00:07:21.413             hex: 00 01 02 00
00:07:21.413 line:5/0 L3 rx ALERTING callref:8.
00:07:21.413             hex1: 08 01 88 01 1e 02 81 82
00:07:21.413 line:5/0 L1 frame sent.
00:07:21.413 line:5/0 L2 tx RR P/F=0 NR=2 NS=2 C/R=0.
00:07:21.413             hex: 00 01 01 04
00:07:25.349 line:5/0 L1 frame received.
```

The user hangs up the handset

```
00:07:25.350 line:5/0 L2 rx I P/F=0 NR=0 NS=2 C/R=0.
00:07:25.350             hex: 00 01 04 00
00:07:25.350 line:5/0 L3 rx CONNECT callref:8.
00:07:25.351             hex1: 08 01 88 07 4c 06 01 80 33 30 33 36
00:07:25.351 line:5/0 L1 frame sent.
00:07:25.351 line:5/0 L2 tx RR P/F=0 NR=3 NS=2 C/R=0.
00:07:25.351             hex: 00 01 01 06
00:07:25.374 line:5/0 L1 frame sent.
00:07:25.374 line:5/0 L2 tx I P/F=0 NR=3 NS=0 C/R=1.
00:07:25.374             hex: 02 01 00 06
00:07:25.374 line:5/0 L3 tx CONNECT ACK callref:8.
00:07:25.374             hex1: 08 01 08 0f
```

RR polling during the call

```
00:07:25.391 line:5/0 L1 frame received.
00:07:25.392 line:5/0 L2 rx RR P/F=0 NR=1 C/R=1.
00:07:25.392             hex: 02 01 01 02
00:07:35.380 line:5/0 L1 frame sent.
00:07:35.381 line:5/0 L2 tx RR P/F=1 NR=3 NS=0 C/R=1.
00:07:35.381             hex: 02 01 01 07
00:07:35.394 line:5/0 L1 frame received.
00:07:35.394 line:5/0 L2 rx RR P/F=1 NR=1 C/R=1.
00:07:35.394             hex: 02 01 01 03
```

Remote disconnection

```
00:07:38.666 line:5/0 L1 frame sent.
00:07:38.666 line:5/0 L2 tx I P/F=0 NR=3 NS=1 C/R=1.
00:07:38.666             hex: 02 01 02 06
00:07:38.666 line:5/0 L3 tx DISCONNECT callref:8.
00:07:38.666             hex1: 08 01 08 45 08 02 80 90
00:07:38.690 line:5/0 L1 frame received.
00:07:38.690 line:5/0 L2 rx RR P/F=0 NR=2 C/R=1.
00:07:38.690             hex: 02 01 01 04
00:07:38.748 line:5/0 L1 frame received.
00:07:38.748 line:5/0 L2 rx I P/F=0 NR=2 NS=3 C/R=0.
00:07:38.748             hex: 00 01 06 04
00:07:38.748 line:5/0 L3 rx RELEASE callref:8.
00:07:38.749             hex1: 08 01 88 4d 08 02 81 90
00:07:38.749 line:5/0 L1 frame sent.
00:07:38.749 line:5/0 L2 tx RR P/F=0 NR=4 NS=1 C/R=0.
00:07:38.749             hex: 00 01 01 08
00:07:38.752 line:5/0 L1 frame sent.
00:07:38.753 line:5/0 L2 tx I P/F=0 NR=4 NS=2 C/R=1.
00:07:38.753             hex: 02 01 04 08
00:07:38.753 line:5/0 L3 tx RELEASE COMPLETE callref:8.
00:07:38.753             hex1: 08 01 08 5a 08 02 81 90
00:07:38.773 line:5/0 L1 frame received.
00:07:38.773 line:5/0 L2 rx RR P/F=0 NR=3 C/R=1.
00:07:38.774             hex: 02 01 01 06

00:07:48.761 line:5/0 L1 frame sent.
00:07:48.761 line:5/0 L2 tx RR P/F=1 NR=4 NS=2 C/R=1.
00:07:48.761             hex: 02 01 01 09
00:07:48.775 line:5/0 L1 frame received.
00:07:48.775 line:5/0 L2 rx RR P/F=1 NR=3 C/R=1.
00:07:48.775             hex: 02 01 01 07
```

Layer 2 disconnection

```
00:07:53.742 line:5/0 L1 frame sent.
00:07:53.742 line:5/0 L2 tx DISC P/F=1 NR=4 NS=2 C/R=1.
00:07:53.742             hex: 02 01 53
00:07:53.757 line:5/0 L1 frame received.
00:07:53.758 line:5/0 L2 rx UA P/F=1 C/R=1.
00:07:53.758             hex: 02 01 73
```

8.3.3 Call Generator/Responder

The call generator enables to place calls automatically without voice terminals. This function makes it easier to validate and troubleshoot the installation of the VoIP router.

Main features:

- Defines a responder number: when the OneOS-based voice-capable router receives a call with this called number, it responds automatically to the call and provides a BERT or Loop service.
- Provides CLI commands to initiate a call with a specific origin & destination number.
- Performs loop mode, BERT testing (BERT: Bit Error Rate Test for unrestricted data service over IP) or voice message generation with a test call.

- Provides CLI commands to enhance setting of advanced features such as:
  - Periodic call generation.
  - Multiple call generation & answering.

8.3.3.1 Responder

8.3.3.1.1 Configuration

The easiest method is to define a new dial-peer voice POTS, which is not attached to a physical port, but which is able to provide a service (loop, BERT, voice message).

Syntax:

```
dial-peer voice pots <pots-id>
 service { loop | bert2047 { both | analyse | sending } | voice-message }
[<number-of-simultaneous-calls>]
 pots-group <id>
 port 5/<x>
exit
```

Note:

- Service could be: loop (loopback received voice flow), bert2047 (Bit Error Rate Test), voice-message.
- The bert2047 could be: sending (send unrestricted data), analyze (receive data and determine loss/error) or both.
- Voice-message is used to play-out or record a message file (G.711 format).
- The following optional number specifies the maximum number of simultaneous calls (the next call is rejected if the number of active call has reached this limit). Default: 1

To disable the responder:

```
dial-peer voice pots <pots-id>
 no service {loop | bert2047}
```

8.3.3.1.2 Details about Responder Signaling

The behavior is as simple as possible. The received call (SETUP message) is automatically accepted and a CONNECT message is returned as long as the maximum number of simultaneous call is not exceeded. If exceeded, the responder returns a DISCONNECT message with the following disconnect cause:

```
44 [Requested circuit/channel not available]
```

No timeout is engaged for DISCONNECT procedure. Only the calling port engages nominal disconnection.

According to current route rules, only local (towards local port) calls are available.

8.3.3.1.3 Details about the RTP Flow

Depends on the service configured:

- Loop: received RTP packets are looped after DSP decompression/compression process.
- Bert2047: a BERT pattern is locally generated towards the calling port while received packets are processed in order to generate statistics.
- Voice-message: either a specific frequency is generated or better a voice-message is locally generated.

8.3.3.2 Call Generator

Two CLI commands are defined to initiate a call: Quick Mode and Multi-Session Mode.

Quick mode

A single CLI command (under the root) initiates a call.

Note: as of V4.3R2E2 software release, `auto-call` command is deprecated and replaced by `test-call` command described hereunder.

```
CLI> test-call called <called> [calling <calling>] [pots <pots-number>]
[bc <bearer>] [overlap <overlap>] [mode <mode>] [duration <duration>]
```

Parameters:

- `called`: called number, up to 21 characters (0-9, #, *****)
- `calling`: calling number. (for routing local calls towards 5/x port) , up to 21 characters (0-9, #, *****)
- `pots-number`: local dial-peer pots identifier to be used: [0-29], default: 30 – virtual port
- `bearer`: bearer capability { **`voice`** | **`data`** | **`voiceband`** }, default: **`data`**
- `overlap`: units in milliseconds: [0-2000] (0 no overlap), default: 0
- `mode`: result mode { **`asynchronous`** | **`synchronous`** }, default: **`asynchronous`**
- `duration`: units in seconds [10-1000000], default: 10

Deprecated command:

```
CLI> auto-call <called> <calling> <pots-number> { voice | data
                                                | voiceband }
```

The `auto-call` default parameter values are the same as the `test-call` command.

Multi-session mode

A CLI command set enables the configuration of several calling sessions.

```
CLI(configure)> voip-call <identifier>
CLI(voip-call)> pots <pots number>
CLI(voip-call)> called <number>
CLI(voip-call)> calling <number>
CLI(voip-call)> bearer { voice | data | voiceband }
CLI(voip-call)> duration <0–1000000>
CLI(voip-call)> timeout <0–1000000>
CLI(voip-call)> start [auto]
CLI(voip-call)> stop [auto]
```

To remove a session:

```
CLI(configure)> no voip-call <identifier>
```

N.B.: `identifier` is an ASCII string limited to 16 characters.

Parameters:

- `pots`: specifies the pots port to be used. The ‘dial-peer voice pots’ is a virtual pots and MUST NOT be bound to a physical port. **The port must not be configured within ‘dial-peer voice pots’. The dial-peer voice pots remains ‘shutdown’.**
- `called`: called number, up to 21 characters (0-9, #, *****, **.**).
- `calling`: calling number (useful for local calls towards 5/x port for routing process).
- `bearer`: bearer capability.
- `duration`: call duration after connection (units in seconds).
- `timeout`: time between the end of a call and the start of the next one (units in seconds).

- `start [auto]`: start the call. The `auto` option allows starting automatically after a reboot.
- `stop [auto]`: stop the call. The `auto` option removes the automatic starting after a reboot.

By default, pots port is 0, call duration to 20 seconds and timeout to 10 seconds. If not defined, bearer is fixed to data. Several test call sessions can be configured simultaneously (with voip-call only).

8.3.3.2.1 Details about Generator Signaling

The behavior is as simple as possible. Only en-bloc dialing is supported. The call (SETUP message) is automatically sent after the "timeout" value specified in the `voip-call` command.

When the call duration is over, a local disconnection (DISCONNECT) with normal cause value (16) is generated. When the timeout is over, a call (SETUP message) is automatically sent, and so on and so on.

If duration is equal to 0, the call is established and remains established forever until the STOP command disconnects the call.

According to current route rules, local (towards local port) or remote (towards dial-peer voip) calls are available.

8.3.3.2.2 Details about Generator Call Type (Service)

Loopback

If the loopback service is defined, all the received voice frames are sent back to the originator.

If the voice information comes from a local port, the voice switching matrix is configured to loopback the G.711 samples.

If the voice information comes from a VoIP port, the voice RTP frames are uncompressed, the matrix is configured to loopback the G.711 samples to the DSP, the voice information is compressed again before sending the RTP frames back to the originator.

BERT 2047

If enabled, the OneOS-based voice-capable router sends a BERT2047 sequence towards the remote end and tests the BERT sequence received from the remote end.

Results are given in the statistics and with periodic events.

A voice message, defined in a file, can be played out or recorded. The main application is voice quality monitoring.

Voice-Message configuration:

```
service voice-message { play | record } <filename> <value>
```

`filename`: voice file name without extension (`.alaw`).

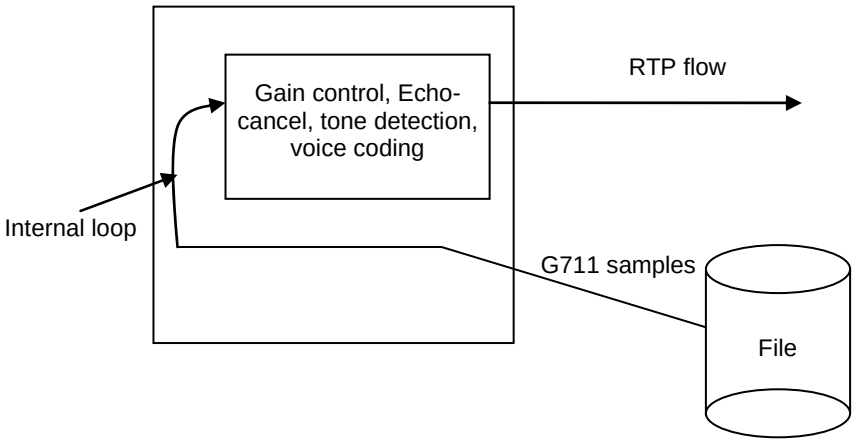
`value`:

- Number of times the message must be played out (0: continuous).
- Maximum time of recording in record mode (1 – 180 seconds).

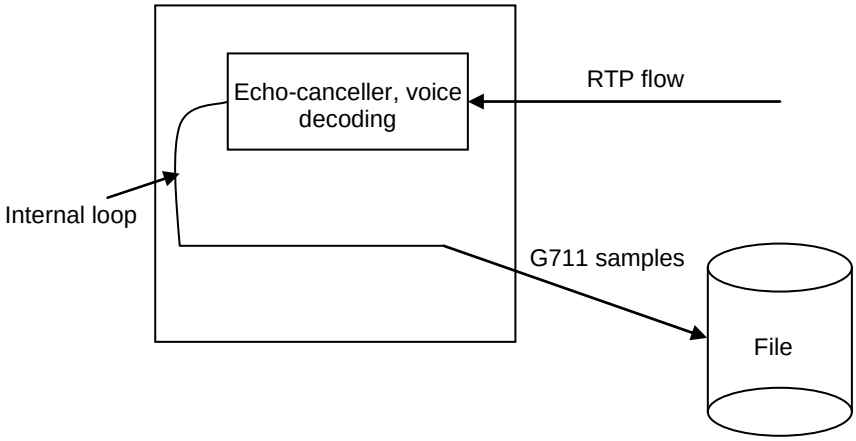
The file is stored in the flash file system (root directory) with the "`.alaw`" extension. The file contains G.711 A-law samples in raw mode. It can be read (or created) on PC by any specialized audio application. The file size is equal to play-out duration x 1KB.

The coder used in the message file is G.711 A-law. It means that, in case of RTP using G729a, an encoding or decoding is performed after the play-out or before the recording.

For the play-out function, the message is processed by the DSP exactly as voice samples received from the pots device:



For the recording function, the message is decoded as any RTP flow and then stored in a file in G.711 A-law format:



Voice Message

Either a specific frequency is generated or, better, a voice-message is locally generated.

8.3.3.2.3 Example

Call Generator:

```
hostname CALL-GENERATOR
dial-peer voice pots 6
 pots-group 6
 service bert2047 both 2
 no shutdown
exit
dial-peer voice voip 0
 sig-protocol sip
 gw-ip-address 20.223.1.2
 no shutdown
exit
voip-call test
 called 7777
 calling 2221111003
 pots 6
 bearer voice
 overlap 0
 duration 10
 timeout 5
exit
```

```
voice-routing
route 10
  dial-peer voip 0
  prefix 7777  length 4
  prefix-type outgoing called last
 exit
exit
```

Call Responder:

```
dial-peer voice pots 5
 pots-group 5
 service  loop 2
 no shutdown
exit
voice-routing
 route 2
  dial-peer pots-group 5
  prefix 217777  length 6
  prefix-type outgoing called last
 exit
exit
```

8.3.3.3 Statistics

8.3.3.3.1 Events

Some specific events were added for call simulator.

Events are activated by the CLI command: `event filter add vox factory all mem`

Example:

```
Info VOX FACTORY Test 1 call-id: 13, ident: appel1, CALL IN PROGRESS
Calling=3000 Called=3003.
Info VOX FACTORY Test 1 call-id: 14, CALL CONNECTED.
Info VOX FACTORY Test 1 call-id: 13, ident: appel1, CALL CONNECTED.
Info VOX FACTORY Test 1 call-id: 13, ident: appel1, Generate BERT
Info VOX FACTORY Test 1 call-id: 14, Begin test BERT
Info VOX FACTORY Test 1 call-id: 14, TEST BERT OK
Info VOX FACTORY Test 1 call-id: 13, ident: appel1, CALL OK with codec
g711a.
Info VOX FACTORY Test 1 call-id: 13, ident: appel1, CALL DISCONNECTED on
pots cause=[Normal call clearing].
Info VOX FACTORY Test 1 call-id: 14, CALL DISCONNECT on voip
cause=[Normal call clearing].
```

8.3.3.3.2 Displaying Statistics

A specific `show` command is added:

```
CLI> show voice voip-test

Outgoing call tests

test-id   pots  status  outgoing  failed  bert_ko
   1       4    running  12345    23      7
   2       4    running  7865     120     50

Incoming call tests

pots  incoming  rejected   bert_ko
  5    12345      23       6
  5    7865       120      80
```

8.3.4 RTP Call Detailed Reports

The RTP session monitoring feature gives history information about MOS, jitter, and packet loss. The last 200 calls and the current calls are monitored.

To display the statistics:

```
CLI> show voice rtpcall { short | full } { any | err }
                              { all | min <val1> max <val2> | ind <value> }
```

Two modes are available:

- `short`: statistics summary.
- `full`: all the statistics.

A filter can be applied to get only the calls with errors: `any` or `err`.

The calls are numbered as following: the 1st is the most recent one and the last call is the oldest one. The first calls can be in progress or not.

Several options are available to select the calls:

- `all`: all the calls from 1 to 100.
- `min <value1> max <value2>`: all the calls between value1 and value2.
- `ind <value>`: the call specified by the value.

Example:

```
CLI> show voice rtpcall short any min 1 max 3

  1 – 01/04/01 00h47m43s RTP 20.5.3.131:16418 – 200.15.0.152:16390
      Play time (voice) : 00h00m47s
      Tx Coder : G729 / 20 ms ; Rx Coder : G729
      RTP Packets RX / TX : 2338 / 2337
      RTP Packet lost&discarded RX / TX (RTCP reported) : 0 / 0
      Number of Excessive Jitter events : 1
      MOS-CQ / MOS-LQ : 3.95 / 4.00

  2 – 01/04/01 00h47m24s RTP 20.5.3.131:16416 – 200.15.0.152:16388
      Play time (voice) : 00h00m46s
      Tx Coder : G711 1 Law / 20 ms ; Rx Coder : G711 A Law
      RTP Packets RX / TX : 2337 / 2338
      RTP Packet lost&discarded RX / TX (RTCP reported) : 0 / 0
      Number of Excessive Jitter events : 1
      MOS-CQ / MOS-LQ : 4.30 / 4.35

  3 – 01/04/01 00h47m05s RTP 20.5.3.131:16414 – 200.15.0.152:16476
      Play time (voice) : 00h00m00s
      Tx Coder : -- / -- ms ; Rx Coder : --
      RTP Packets RX / TX : 0 / 0
      RTP Packet lost&discarded RX / TX (RTCP reported) : 0 / 0
      Number of Excessive Jitter events : 0
      MOS-CQ / MOS-LQ : -- / --
```

In full mode:

```
CLI> show voice rtpcall full any index 2

  2 – 01/04/01 00h47m24s RTP 20.5.3.131:16416 – 200.15.0.152:16388
      Play time (voice) : 00h00m46s
      Tx Coder : G729 / 20 ms ; Rx Coder : G729
      VAD enabled local / remote : no / no

      ERL   : 32 dB
      ACOM  : 67 dB
      MOS-CQ   : 3.95
```

```
      MOS-LQ   : 4.00
      remote MOS-CQ   : 3.90
      remote MOS-LQ   : 3.90

R
    79|**************************
    77|
     ------------------------------
                              30 mn

      RTP Packets received (DSP / Uplink) : 2337 / 2337
           lost : 0
           out of sequence : 0
           invalid : 0
      RTP Packets transmitted (DSP / Uplink) : 2338 / 2338
           lost (RTCP reported) : 0

      Jitter parameter : 100 ms
      Number of Excessive Jitter events : 1

      Excessive Jitter events :
 2|
 1|  *
  ----------------------------------------
      0  30"   1'   2'   4'   8'  12' >16'



      Jitter received (uplink) :
           Max delay : 93 ms
           Delays (ms)     >50  >100  >150  >200  >300
           Nb of occur.      2     0     0     0     0
           Interarrival max jitter : 9 ms
      Jitter received (DSP) :
           Max delay : 93 ms
           Delays (ms)     >50  >100  >150  >200  >300
           Nb of occur.      2     0     0     0     0
           Interarrival max jitter : 9 ms

      Frames with a delay >50 ms :
 2|
 1|  *    *
  ----------------------------------------
      0  30"   1'   2'   4'   8'  12' >16'

      Jitter transmitted (uplink) :
           Max delay : 6 ms
           Delays (ms)     >50  >100  >150  >200  >300
           Nb of occur.      0     0     0     0     0
           Interarrival max jitter : 1 ms
                   (RTCP reported) : 2 ms
```

Notes:

- ERL is the Echo Return Loss measured before echo cancellation. ACOM is the echo return loss measured after echo cancellation.
- MOS-CQ is the Mean Opinion Score Conversational Quality. MOS-LQ is the Mean Opinion Score Listening Quality. Remote MOS-CQ and MOS-LQ are the values as calculated by the remote end.
- When a value has not been calculated, it is replaced by a "–". Examples: uplink analysis is disabled, the ERL & ACOM when an echo situation has not been encountered (an echo situation is a high transmitted audio signal and low received audio signal), no RTCP packets received.
- A graph indicates the time distribution of the errors. The 30 sec column indicates the number of errors occurred between 30 sec and 1 min after the beginning of the call.

- For the jitter statistics, “delay” means the time between two packets decreased by the normal time. Example: a delay of 80ms for a 20ms coder sample length causes a jitter of 60ms towards expected value.
- The inter-arrival jitter is calculated for each packet in conformance with the RFC3550. The indicated value is the max jitter observed during the call.
- A graph indicates the time distribution of the R factor minute by minute for the last 30 minutes of the call.

8.3.5 VoIP Call Detailed Reports

A history of the last VoIP calls is offered with the information about:

- Date &Time & Duration.
- Calling & Called number.
- Inbound & Outbound ports.
- Cause of disconnection.
- Summary of the RTP sessions.

To display the statistics:

```
CLI> show voice voip-call { any | err } { all | min <val1> max <val2>
                                                    | ind <value> }
```

Example:

```
CLI> show voice voip-call any all

1 – Call from voip-group: 1 (Uplink), to voip-group: 0  call-id: 167 (44)
     calling : 7071, called : 0141877049
     setup time:  23/01/08 12h42m02s
     connexion time: 23/01/08 12h42m06s
     disconnected by remote voip: 1 cause ☹16)[Normal call clearing]
     call duration: 00:01:08

 23/01/08 12h42m03s
     RTP  Source  ip  :192.168.0.10  rtp:16438  /Dest  ip  :192.168.0.20
rtp:16402
     Play time (voice) : 00h01m08s
     Tx Coder : G711 A Law / 40 ms ; Rx Coder : G711 A Law
     RTP Packets RX / TX : 1783 / 1784
     RTP Packet lost&discarded RX / TX (RTCP reported) : 0 / 0
     Number of Excessive Jitter events : 0

 2 – Call from voip-group: 1 (Uplink), to voip-group: 0  call-id: 165
(40)
     calling : 149288663, called : 0141877053
     setup time:  23/01/08 12h20m11s
     connexion time: 23/01/08 12h20m14s
     disconnected by remote voip: 1 cause ☹16)[Normal call clearing]
     call duration: 00:15:10

 23/01/08 12h20m12s
     RTP  Source  ip  :192.168.0.10  rtp:16434  /Dest  ip  :192.168.0.20
rtp:16398
     Play time (voice) : 00h15m10s
     Tx Coder : G711 A Law / 40 ms ; Rx Coder : G711 A Law
     RTP Packets RX / TX : 22805 / 22807
     RTP Packet lost&discarded RX / TX (RTCP reported) : 0 / 0
     Number of Excessive Jitter events : 0
```

8.3.6 Protocol Traces

Note: The following commands activate traces for debugging purpose only (they will be interpreted and analyzed by OneAccess employees. OneAccess does not provide any explanation for those traces):

The following command displays the voice memory usage recap (default all):

```
CLI> show voice debug memory [appli | netb | all]
```

The following command defines which voice memory usage is to be displayed:

```
CLI> debug voice memory [off | appli | netb | all]
```

The following command displays the graph of voice memory usage over time (default all):

```
CLI> show voice debug memory-graph [appli | netb | all]
```

The following command defines the format of the graph (default peak for 3600 seconds):

```
CLI> debug voice memory-graph { peak | average } <100..36000>
```

The following command displays the number of VoIP contexts:

```
CLI> show voice debug voip-comm
```

The following command displays the VoIP sessions contexts:

```
CLI> show voice debug voip-session
```

The following command displays (or reset) SIP stack counters:

```
CLI> show voice debug sip-stack [<reset>]
```

The following command, in global voice configuration mode, activates tracing the messages exchanged by VoIP sessions:

```
CLI> configure terminal
CLI(configure)> voice-global
CLI(voice-global)> [no] audit voip-session enable
CLI(voice-global)> exit
CLI(configure)> exit
CLI>
```

The status `enable` or `disable` (default) can be displayed using:

```
CLI> show voice audit
```

The exchanged messages are displayed using:

```
CLI> show voice debug message-exchanges
```

The following command activates SIP traces:

```
CLI> [no] debug sip
```

The following command activates H.323 traces:

```
CLI> [no] debug h323
```

9 SIP PROXY

The main functions of the SIP proxy are:

- To deliver local SIP call switching in case of network failure (softswitch not reachable).
- To provide an extended NAT SIP ALG.
- To manage SIP calls with SIP-IP phones (wired or wireless IP phones).

9.1 INTRODUCTION TO SIP PROXY

Let us take an example: SIP phones are connected to an OneOS-based voice-capable router. SIP phone call control should be managed by a softswitch. However, it is desired to hide the softswitch by the OneOS SIP proxy. The SIP phones talk to the SIP proxy, which makes the decision to switch the SIP call to another destination. Call switching refers to routing a call to an appropriate destination: the softswitch, or a local port (ISDN, FXS interfaces), or another IP phone attached to the LAN interface of the router. The SIP proxy can be configured such that the calls can be routed locally in case of connection loss to the softswitch.

In the SIP terminology, the OneOS SIP proxy works as a B2B UA (Back-to-Back User Agent), which means it has got a user agent server interface (to receive calls from SIP phones) and a user agent client interface to place calls directed to the softswitch. The user agent client interface is actually the SIP gateway.

9.1.1 Registrar and Registration to Softswitch

The embedded registrar maintains a mapping table between the IP phone numbers and their dynamic IP addresses. The registrar is attached to one logical IP interface, such as the LAN interface. In other words, the OneOS-based voice-capable router can route a call to an IP phone, once the IP phone has registered. Otherwise, it is not able to locate the IP phone.

When an IP phone registers, OneOS (if configured so) checks phone number and authentication data.

The IP phone registration is not translated into a REGISTER message sent to the softswitch. The OneOS router registers all registered phone number to the softswitch.

9.1.2 Call Routing

Call routing re-uses the voice-routing module common to H.323 and SIP- gateway.

If the SIP gateway is down (see '`show voice sip-gateway`'), the backup mode is enabled. One can envisage that the preferred path for call routing is to switch the call through the softswitch. In backup mode, calls can be switched by the SIP proxy, thereby enabling local calls while the softswitch cannot be reached.

9.1.3 SIP Signaling Translation

SIP signaling is processed by the SIP proxy, such that IP phone IP address is replaced by the router IP address. The change is done within "Contact" and "From" header fields (if the fields are not FQDN).

If the SIP messages contain SDP information, the IP phone IP addresses are replaced by the router public IP address.

The SIP proxy is due to be transparent to SIP advanced voice features controlled by the softswitch or the IP phones.

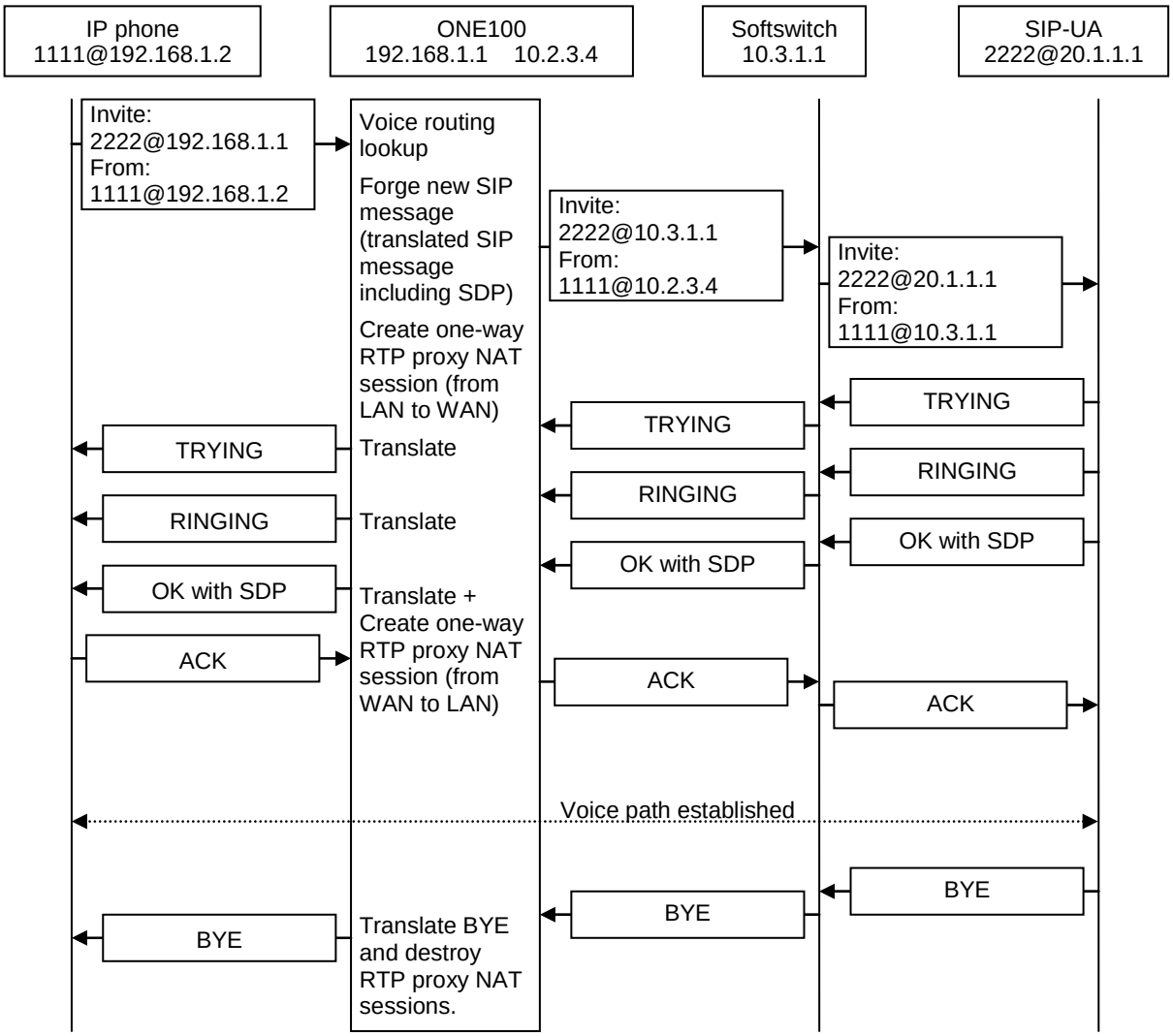
9.1.4 NAT ALG

On an interface where dynamic NAPT address translation is enabled, some protocols cannot function properly. The reason is that those protocols negotiate the opening of ports dynamically without being aware that the ports are not open by default by the NAPT function. A NAT Application Level Gateway is a function that inspects a protocol at the application level and extracts some interesting information to control the opening of ports within the NAPT module.

The RTP proxy manages IP address/port translation for RTP flows. Local calls managed by the softswitch require that RTP flows be switched by the RTP proxy. In other words, local calls require router CPU. So the number of simultaneous calls managed by the router must be kept at a level allowed by the CPU.

9.1.5 Basic Call Flow

The standard case is that the SIP proxy acts as a relay for SIP signaling. Let us take an example first. The OneOS-based voice-capable router has got a LAN interface (192.168.1.1/24) and a WAN interface (10.2.3.4). The softswitch IP address is 10.3.1.1.



9.2 SIP PROXY CONFIGURATION COMMANDS

The SIP proxy is tightly integrated into SIP gateway architecture. In other words, the reader of the document should first master SIP gateway configuration before starting to configure the SIP proxy.

The configuration steps are the following:

- SIP server interface: configuration of SIP UA server and registrar.
- VoIP dial-peer: configuration of SIP end-points.
- Voice-routing: definition of rules for call switching rules and preference. The information for authenticating registration is configured in voice-routing.

9.2.1 SIP Server

The SIP UA server must be configured to attach it to an IP address and configure the embedded registrar for IP phones.

To enter in sip-server configuration mode and attach an IP:

```
CLI(configure)> sip-server
CLI(sipserv)> interface { fastEthernet <x>/<y> | bvi <id> | … }
```

The registrar can be enabled as follows:

```
CLI(sipserv)> [no] registrar-hostname <string>
CLI(sipserv)> registrar { required | optional }
```

The registrar-hostname is the name used, instead of the IP address, to fill the CONTACT field of the 200OK answer. The required mode indicates that the IP phone must be provisioned prior to registering. The optional mode allows the IP phone to register without being provisioned. To disable the registrar:

```
CLI(sipserv)> registrar disabled
```

The RTP port range and SIP signaling port can be configured as follows (default sig. Port UDP 5060):

```
CLI(sipserv)> call-sig-port <udp-port>
CLI(sipserv)> rtp-port-range <min> <max>
```

By default, the SIP server replies 200 OK to legitimate REGISTER requests with an expiration timer equal to the requested expiration time. However, you can force this timer to a customized value:

```
CLI(sipserv)> reg-ka <seconds>
```

Use the following command to force the state of the number portability function. The timeout parameter is optional and specifies the duration of the "in-progress" state. The default value is 5760 minutes (4 days). Use the no form to disable the portability function (default).

```
CLI(sipserv)> set-portability { enable | in-progress | done }
                                    [timeout <time-in-minutes 1-525600>]
```

Finally the SIP server must be activated as follows:

```
CLI(sipserv)> no shutdown
CLI(sipserv)> exit
```

9.2.2 VoIP dial-peers

From the signaling perspective, there is no difference in SIP protocol if the VoIP peer is a softswitch or a standard user agent (like an IP phone). Therefore, IP phones are declared as VoIP dial-peers like the softswitch. However, the difference is that OneOS may not know the IP address of such dial-peers in advance. Some extra attributes under `dial-peer voice voip` are added to designate dial-peer whose IP is learnt through a registration process.

First enter in `dial-peer voice voip` configuration mode:

```
CLI(configure)> dial-peer voice voip <0..7>
CLI(voip)> sig-protocol sip
```

Then, the SIP UA type must be explicitly defined in case of an IP phone:

```
CLI(voip)> sip-ua { ip-dynamic { restricted | open }
                  | ip-static <A.B.C.D> | mac-static <aa:bb:cc:dd:ee:ff> }
```

Explanation of the various modes: Several application cases are supported:

- IP phones without configuration (except SIP proxy & registrar IP address): in such case, the IP Phone is identified by its IP address or MAC address. The `ip-static` or `mac-static` mode will be used and a `dial-peer voip` will be defined for each IP phone. If the registration process is used, the phone number is configured in the voice routing table: the sip id or the phone number that is indicated by the IP phone is not taken into account. In that case, you must configure **as much dial-peers as IP phones**.
- IP phones with a configured phone number are able to support registration: in such case, **a single dial-peer VoIP** is defined in `ip-dynamic` mode. In this mode, two behaviors are possible :
  - Restricted mode (default): the phone number must be configured in the routing table. If not, the register request is refused.
  - Open mode: an entry is automatically created in the routing table for each IP phone (not saved if reboot or power-off).

To complete the dial-peer configuration:

```
CLI(voip)> exit
```

9.2.3 Voice-Routing

You can define in voice-routing the preferred call switching path for IP phones.

To enter in voice-routing configuration mode and create a voice route:

```
CLI(configure)> voice-routing
CLI(voice-route)> route <1..200>
CLI(conf-voice-route)>
```

Then, associate a phone number to the IP phone '`dial-peer voice voip`' configured before:

```
CLI(conf-voice-route)> prefix <phone-nbr> length <length>
CLI(conf-voice-route)> dial-peer voip <voip-dial-peer-id> ua-sip
```

You can define authentication:

```
CLI(conf-voice-route)> sip-uas-authentication <username> [<password>]
                                                         [<type>]
```

If the command above is entered, authentication is mandatory for registration request coming from IP phones while the command `sip-authentication` serves to authenticate the registration of the OneOS-based router to the softswitch registrar. In other words, the username/password used for authentication on IP phone and softswitch side can be different. The optional parameter `type` allows hiding the password in the CLI text file and for a `show running-config` command. `type 0` indicates that the password must be encrypted. `type 1` indicates that the password is already encrypted. If the parameter `type` is absent then the password is unchanged (not encrypted).

Not all commands under voice-routing are detailed here. Please refer to 7.2.

Finally, complete the configuration as follows

```
CLI(conf-voice-route)> exit
CLI(voice-route)> exit
```

9.2.4 SIP Proxy with Transcoding Capability

By default, the RTP packets are NAT-ted if the RTP stream is sent over NAT-ted SIP gateway interface. In that case, the SIP proxy modifies the SDP part of SIP signaling like a SIP NAT ALG.

OneOS SIP proxy supports also an RTP proxy that makes it possible to transcode an RTP stream (example: G.711 on LAN to G.729 on WAN, G.711 on LAN to T.38 on WAN). In that case, a call is split into two independent LAN and WAN call legs. The RTP streams are terminated in OneOS DSP, where they are decoded and then encoded in the codec of the other call leg.

Benefits of RTP proxy:

- Consistent media behavior seen by the SIP network (codec negotiation, DTMF…), independently from the IP-PBX behind the OneOS-based voice-capable router.
- Solves interoperability issues with T.38.

Drawback of RTP proxy:

- A proxied call without transcoding takes approximately as much DSP resources as making one G.729 call from the SIP gateway. Without RTP proxy, no DSP resource is involved. The default mode is to not use the RTP proxy.

To set the default mode (without RTP proxy):

```
CLI(configure)> voice-global
CLI(voice-global)> sip-proxy bridge
```

To have the SIP proxy (without RTP proxy) being fully transparent to SIP messages (including REGISTER and SUBSCRIBE messages):

```
CLI(voice-global)> sip-proxy bridge-transparent
```

In this mode all dial-peer VoIP configured in `ua-sip` are not registered to the external registrar.

To enable the RTP proxy:

```
CLI(voice-global)> sip-proxy back-to-back
```

If RTP proxy is enabled, the VoIP coder profile as well as the modem/fax handling must be set on the VoIP dial-peers. Example:

```
configure terminal

! dial-peer with IPBX
dial-peer voice voip 0
 sig-protocol sip
 fax-relay passthrough
 modem-passthrough
 passthrough-mode reinvite
 voip-coder-profile 0
 no shutdown
exit

! dial-peer with SIP application server (external trunk)
dial-peer voice voip 1
 sig-protocol sip
 dtmf-relay in-band
 fax-relay t38
 modem-passthrough
 passthrough-mode reinvite
 voip-coder-profile 1
 no shutdown
exit

exit
```

9.2.5 Statistics and Debug

To activate the SIP server debug traces (displays the information extracted from SIP signaling on the SIP server side), enter the following command:

```
CLI> debug sip-registrar packet all
```

To disable the traces, enter `no debug`. The raw SIP signaling is viewed by means of the 'debug sip' command.

To display the status of the SIP UA Server, enter the next command:

```
CLI> show voice sip-server
        Sip-Server statistics :
        Server state                    up
        Registration requests           2
        Registrar server                192.100.100.1:5060

        Current call                    0
```

To display the SIP phones currently registered with the internal SIP Server, use the next command:

```
CLI> show voice sip-server endpoints

        phone 3 :
                Number : 2409995773
                IP address : 192.100.100.150
                SIP-id : 2409995773
                Registration time : 1h 50m 14s
                Registration timeout : 396s/600s

        phone 5 :
                Number : 2409995774
                IP address : 192.100.100.12:5060
                SIP-id : 2409995774
                Registration time : 1h 50m 15s
                Registration timeout : 572s/600s
```

To display the phone numbers of the SIP gateway currently registered with the softswitch, use the next command:

```
CLI> show voice sip-gateway endpoints
```

If you are passing calls through the SIP proxy and NAT is required, the corresponding sessions appears in the NAT session table. See the next 'show' command:

```
CLI> show ip nat sessions
```

The following commands activate traces for debugging purpose only (they will be interpreted and analyzed by OneAccess employees. OneAccess does not provide explanation for those traces):

```
CLI> trace filter add vox voiproute 2 show       ! voice routing
CLI> trace filter add vox sip autom 2 show       ! SIP protocol
CLI> trace filter add vox up ifp 2 show          ! T.38
```

9.2.6 Configuration Example

In this configuration example, the softswitch is reached via its IP address 200.15.0.53 via the atm 0.1 interface. Two IP phones are configured: they have a dynamic IP address and have the phone number 1111 and 2222. The IP phones register to the OneOS-based voice-capable router via the LAN interface:

```
! Dial-peer for softswitch
dial-peer voice voip 0
 sig-protocol sip
 gw-ip-address 200.15.0.53
 voip-coder-profile 0
 no shutdown
```

```
exit
! Dial-peer for IP phones
dial-peer voice voip 1
 sig-protocol sip
 voip-coder-profile 0
 sip-ua ip-dynamic restricted
 no shutdown
exit
voice-routing
! First route: call is switched by softswitch
! If softswitch is not present
 route 10
  dial-peer voip 0
  prefix .  length 4
  prefix-type outgoing called backup
  no loopback-routing
 exit
 route 11
  dial-peer voip 1 ua-sip
  sip-authentication  user1 password1
  prefix 1111  length 4
  prefix-type outgoing called last
  loopback-routing
 exit
 route 12
  dial-peer voip 1 ua-sip
  sip-authentication  user2 password2
  prefix 2222  length 4
  prefix-type outgoing called last
  loopback-routing
 exit
exit
sip-gateway
 gw-interface atm 0.1 intrusive
 reg-ka 120
 reg-dns-add 200.15.0.33
 device-host-name mydomain.com
 uri-contact ip-address
 no shutdown
exit
sip-server
 interface fastethernet 0/0
 registrar required
 registrar-hostname mydomain.com
 no shutdown
exit
```

10 CALL ADMISSION CONTROL (CAC)

10.1 INTRODUCTION TO CAC

The Call Admission Control (CAC) is a feature that is involved to accept incoming and outgoing call. It makes sure that enough bandwidth is available before call establishment on an interface in order to sustain voice quality after call establishment.

CAC is available for SIP gateway, H.323 gateway and SIP server.

RTP is the real time protocol transporting voice: the required bandwidth for each voice call must be available. To calculate the bandwidth, all the elements of a packet must be considered:

- Voice payload (see table hereafter).
- IP/UDP header: 28 bytes.
- RTP header: 12 bytes.
- IP encapsulation in the WAN interface: it depends on the interworking protocol.
- If applicable, ATM AAL5 encapsulation (depending on the packet length).

Units in the table: Period sampling in milliseconds, Length in bytes, Bandwidth: in bit per second (bps).

			Length		**Bandwidth requirements**		
	Period	*Packet/sec*	*Voice only*	*with IP*	*IP only*	*Ethernet*	*ATM*
G.711/CES	10	100	80	120	96000	126400	127200
	20	50	160	200	80000	95200	106000
	30	33.33	240	280	74659	84792	84792
	40	25	320	360	72000	79600	84800
G.726 32Kbps	10	100	10	50	64000	94400	84800
	20	50	20	60	48000	63200	63600
	30	33.33	30	70	42662	52795	56528
	40	25	40	80	40000	47600	53000
G729AB	10	100	10	50	40000	70400	84800
	20	50	20	60	24000	39200	42400
	30	33.33	30	70	18665	28797	28264
	40	25	40	80	16000	23600	21200
	60	16.67	40	80	10669	15736	14136

Note: the ATM bandwidth is identical whatever the IP encapsulation IPoA & PPPoA VC-Mux or LLC-Mux because the AAL5 encapsulation overhead and padding is taken into account.

10.1.1 Call Admission

The CAC bandwidth is configured as the layer-2 bandwidth corresponding to `gw-interface` encapsulation. If the `gw-interface` is attached to ATM 0.1 (IPoA encapsulation), G.729@20 ms requires 42.4 kbps (see table above).

When an outbound call is placed (from OneOS-based voice-capable router to VoIP network), the available bandwidth is decremented by the layer-2 bandwidth required by G.711 (or the most bandwidth consuming codec). Taking G.711 is a conservative solution (worst case).

When an inbound call is received (from VoIP network, destined to OneOS-based voice-capable router), the available bandwidth is decremented by the bandwidth corresponding to the requested codec. For example, if a call requires the use of G.729A@20 ms on an ATM interface, the available bandwidth is decremented by 42.4 kbps on an ATM interface. If the call requires that the RTP stream is sent to the LAN (whereas SIP-gateway is attached to another interface such as ATM 0.1), no CAC is performed. This case relates to an IP phone sending its RTP stream directly to the IAD (call between an IP phone and a FXS subscriber). In case of inbound calls, if the SDP in INVITE indicates that the receiver is the IAD itself, this INVITE is always accepted (because it is a local call).

The available bandwidth must be greater than 0 after decrementing available bandwidth, otherwise the call is rejected.

The available bandwidth does not result from sums/subtraction of bandwidth for the various codec. The bandwidth is evaluated dynamically. When the CAC function is called, the used bandwidth is calculated as the effective bandwidth sent by DSP through the gateway interface (such as ATM 0.1) + bandwidth from SIP phones.

The bandwidth is calculated based on interface type which the gateway interface is attached with.

To make things clear, let us imagine an OneOS-based voice-capable router with 2 SIP phones and 2 FXS phones. The SIP-gateway is attached to ATM 0.1 (IPoA encapsulation). The CAC bandwidth is 160 kbps. A G.711 call requires 106 kbps and a G.729 call requires 42.4 kbps.

Active Calls	New Call	CAC Result
1 FXS call (G.729) to VoIP network	1 FXS call to VoIP network	Estimated bandwidth = 1 x G.729 + 1 x G.711 = 148.4 kbps **CAC test passes.**
1 FXS call (G.711) to VoIP network	1 FXS call to VoIP network	Estimated bandwidth = 2 x G.711 = 212 kbps **CAC test fails.**
1 FXS call (G.729) to VoIP network	1 SIP phone call to VoIP network	Estimated bandwidth = 1 x G.729 + 1 x G.711 = 148.4 kbps **CAC test passes.**
1 FXS call (G.711) to VoIP network	1 SIP phone call to VoIP network	Estimated bandwidth = 2 x G.711 = 212 kbps **CAC test fails.**
1 FXS call (G.711) to VoIP network	1 SIP phone call to LAN network	Estimated bandwidth = 1 x G.711 = 106 kbps **CAC test passes.**

10.1.2 Media Renegotiation

When the codec is changed, it is assumed that media re-negotiation takes place; possible methods are:

- H.323 request mode
- H.323 TCS null
- SIP re-INVITE
- Pass through mode (switching directly from G.729 to G.711 without notifying remote party).

The same CAC function is used to accept or reject the media change. When the media is renegotiated, the media change can be rejected if it requires more bandwidth than available and if renegotiation was invoked by SIP re-INVITE or H.323 request mode. In case of H.323 TCS null or pass through mode, the call is released directly if the CAC refuses media change.

10.2 CAC CONFIGURATION AND CONTROL

The maximum allowed bandwidth must be specified as the throughput on the line. It must take into account the RTP stream + RTCP (ca 5% of RTP throughput).

To specify the maximum bandwidth under H.323 gateway:

```
CLI(configure)> h323-gateway
CLI(h323gw)> [no] max-bandwidth <0-2147483647 bps>
```

To specify the maximum bandwidth under SIP gateway:

```
CLI(configure)> sip-gateway
CLI(sipgw)> [no] max-bandwidth <0-2147483647 bps>
```

To specify the maximum bandwidth under SIP server:

```
CLI(configure)> sip-server
CLI(sipserv)> [no] max-bandwidth <0-2147483647 bps>
```

Note that the default value is 2147483647 bits per second (no limitation) for the 3 commands above.

The usable bandwidth used by CAC is by default the bandwidth of the output interface used by the gateway (refer to `gw-interface` command). It is possible to define another interface to retrieve the usable bandwidth with the following commands:

```
CLI(h323gw)> [no] bandwidth-interface <type> <unit>

CLI(sipgw)> [no] bandwidth-interface <type> <unit>

CLI(sipserv)> [no] bandwidth-interface <type> <unit>
```

The recommended solution for the usable bandwidth is to take into account the real gateway interface bandwidth (e.g. ATM 0.1 synchronized with DSL might have various synchronization speeds) using the following commands:

```
CLI(h323gw)> [no] gw-interface-bw-ctrl

CLI(sipgw)> [no] gw-interface-bw-ctrl

CLI(sipserv)> [no] interface-bw-ctrl
```

The Call Admission Control (CAC) is activated using the following commands:

```
CLI(h323gw)> [no] bandwidth-control ratio <ratio%>
                  [rate {current-rate | max-rate}]
                  [switch <number of possible calls switching to g711>]

CLI(sipgw)> [no] bandwidth-control ratio <ratio%>
                  [rate {current-rate | max-rate}]
                  [switch <number of possible calls switching to g711>]

CLI(sipserv)> [no] bandwidth-control ratio <ratio%>
                  [rate {current-rate | max-rate}]
                  [switch <number of possible calls switching to g711>]
```

`ratio` is the percentage of bandwidth available for voice (default: 100%). The CAC is calculated for the following bandwidth:

```
bandwidth = ratio x MIN(max-bandwidth, interface-bandwidth)
```

When the CAC checks if a call can be admitted, it checks that there is enough bandwidth for the new G.711 call (even if the call is finally established in G.729).

If the `rate` parameter is `max-rate`, all active calls are counted as taking the bandwidth of a G.711 call (default behavior corresponding to older OneOS versions). It is mandatory to set the rate parameter as `current-rate` so as the bandwidth of all active calls taken into account by CAC is the real one.

Additionally, if the `switch` parameter is set (default: 0 number of calls switching to G.711), the CAC checks also that there is enough bandwidth for a number of calls upgrading their media to G.711.

The following commands specify that OneOS can choice the type of voice coder to better manage the available bandwidth. Use the `ratio` parameter to define the threshold of the available bandwidth above which the calls are switched from G.711 to G.729A. Refer to 5.2.2 for more information.

```
CLI(H323gw)> [no] dynamic-coder-selection ratio <ratio%>

CLI(sipgw)> [no] dynamic-coder-selection ratio <ratio%>

CLI(sipserv)> [no] dynamic-coder-selection ratio <ratio%>
```

Recommended parameter set for the H.323 gateway:

```
CLI(configure)> h323-gateway
CLI(h323gw)> [no] max-bandwidth <0-2147483647>
CLI(h323gw)> [no] bandwidth-control ratio 100 rate current-rate
CLI(h323gw)> [no] gw-interface-bw-ctrl
CLI(H323gw)> [no] dynamic-coder-selection 90
```

For the SIP gateway:

```
CLI(configure)> sip-gateway
CLI(sipgw)> [no] max-bandwidth <0-2147483647>
CLI(sipgw)> [no] bandwidth-control ratio 100 rate current-rate
CLI(sipgw)> [no] gw-interface-bw-ctrl
CLI(sipgw)> [no] dynamic-coder-selection 90
```

For the SIP server:

```
CLI(configure)> sip-server
CLI(sipserv)> [no] max-bandwidth <0-2147483647>
CLI(sipserv)> [no] bandwidth-control ratio 100 rate current-rate
CLI(sipserv)> [no] interface-bw-ctrl
CLI(sipserv)> [no] dynamic-coder-selection 90
```

A counter for rejected calls can be seen with the command:

```
CLI> show voice dial-peer voice voip <id>
```

Also, media change and call rejection can be seen with event command:

```
CLI> event filter add vox all show
```

11 MEDIA GATEWAY CONTROL PROTOCOL (MGCP)

11.1 INTRODUCTION TO MGCP

The OneOS-based voice-capable router enables the connection of conventional analog telephone terminals, or PBXs (analog), to the PSTN through a VoIP network compliant with MGCP 1.0. The OneOS-based voice-capable router is a voice gateway and interworks with a Call Agent (the softswitch in MGCP terminology).

11.1.1 MGCP Protocol Overview

11.1.1.1 Signaling Processing

The OneOS-based voice-capable router implements the MGCP 1.0 protocol in conformance with:

- IETF RFC 3435, 2705 (MGCP 1.0)
- IETF RFC 2327 (SDP)
- IETF RFC 5347 (FAX package) (draft-andreasen-mgcp-fax)

11.1.1.2 Call Agent

The call agent is defined by its IP address, which is configurable.

The OneOS-based voice-capable router is identified by a configurable string of character. It can be for example a Domain Name, a MAC address (in such case, the MAC address must be entered in ASCII mode).

Each voice port is identified by an endpoint name which is a string of character. The recommended value is "`aaln/x`" where `x` is the port number.

The connection status is reported in the statistics.

11.1.1.3 Tones & ringing

The OneOS-based voice-capable router sends configurable tones & ringing signals, when requested by the call agent.

Several profiles are defined: France, United Kingdom, Germany, Spain, Italy, and USA.

A user-defined profile can be configured as well.

11.1.1.4 Caller Identification

The OneOS-based voice-capable router generates the appropriate information about the caller number during the ringing signal. Two modes are supported: FSK or DTMF. The initial ringing duration is configurable.

11.1.2 Backup

The ONE100 has an optional FXO port for a backup purpose. It can be used to offer a backup service in case of failure on MGCP (uplink down, Call Agent unreachable…).

The operation is as follows:

- Upon a failure on MGCP, a busy tone is sent to all the phones which are in an off-hook state.
- The signaling of the FXS ports is then handled locally by the ONE100 through voice-routing, as described in the H.323/SIP chapter (see 5). It becomes possible to make calls between the FXS ports and the FXO port with an optional emergency procedure.
- If the MGCP call agent becomes reachable, the existing calls on FXS ports are maintained. When the FXS ports come back to on-hook state, they are handled again by the MGCP call agent.

11.1.3 Voice Processing

These coders are supported:

- G.711 A law (64Kbps)
- G.711 u law (64Kbps)
- G.729A (8 Kbps, no silence suppression)
- G.729AB (8 kbps, optional silence suppression)

The RTP/RTCP protocol is used for voice packet transmission.

The transmission periodicity is configurable at 10, 20, 30, 40 ms for G.729A/AB, G.711 and CES. The OneOS-based voice-capable router accepts any periodicity on the reception flow and supports the asymmetric coding mode (for example: transmission in G.729, reception in G.711).

The RTP is a real-time protocol: the required bandwidth for each voice call must be available.

To calculate the bandwidth, all overheads of a packet must be considered:

- Voice payload (see table hereafter)
- IP/UDP header: 28 bytes
- RTP header: 12 bytes
- IP encapsulation in the WAN interface: it depends of the interworking protocol
- If needed, ATM AAL5 encapsulation (depending on the packet length).

Units used in the table:

- Period: sampling in milliseconds
- Length: in bytes
- Bandwidth: in bit per second (bps)

			Length		**Bandwidth requirements**		
	Period	*Packet/sec*	*Voice only*	*with IP*	*Ethernet*	*ATM*	*IP only*
G.711/CES	10	100	80	120	126400	127200	96000
	20	50	160	200	95200	106000	80000
	30	33.33	240	280	84792	84792	74659
	40	25	320	360	79600	84800	72000
G729AB	10	100	10	50	70400	84800	40000
	20	50	20	60	39200	42400	24000
	30	33.33	30	70	28797	28264	18665
	40	25	40	80	23600	21200	16000

Note: the ATM bandwidth is identical whatever the IP encapsulation IpoA & PPPoA VC-Mux or LLC-Mux, because the AAL5 encapsulation overhead and padding is taken into account.

The silence suppression is compliant with the standard referenced in G.729AB. For the other coders (G.711), silence is suppressed using an optional comfort noise generation (the noise level is sent periodically to the remote end) in conformance with RFC3389.

11.1.3.1 Group 3 FAX Processing

Transparent Mode

The G3 FAX can be transported by using G.711 coding. OneOS automatically disables the Echo Canceller if a G3 FAX is detected (optional) or switches the echo-canceller to a specific mode. The G.711 coder can be selected per configuration or dynamically during a voice communication when a modem or FAX is detected: this mode is called "Modem pass through".

FAX Pass through

Two methods can be used:

1. The OneOS-based voice-capable router can directly switch to a G.711 coding mode dynamically during a voice communication when a Group 3 FAX is detected. The Echo Cancellation remains enabled but in a specific mode (for G3 FAX).
2. The OneOS-based voice-capable router informs the Call Agent that a G3 FAX tone is detected. Then the call agent switches the connection to G.711.

FAX Relay

The OneOS-based voice-capable router also supports FAX Relay compliant to ITU-T T.38 (UDP mode). The signal is modulated & demodulated locally, the T.30 messages are analyzed and relayed, and the fax data are transported transparently over IP/UDP. The V.27 ter (4800 bps) and V.29 (9600 bps) modulations are supported. The OneOS-based voice-capable router offers FAX Spoofing to avoid FAX failures in case of long transit delays over IP.

The T.38 session is initiated by the Call Agent when the CPE indicates that a G3 FAX tone is detected.

11.1.3.2 Modem Processing

Transparent Mode

A Modem signal can be transported by using G.711 coding mode. OneOS automatically disables the Echo Canceller if a modem is detected. The G.711 coder can be selected by configuration for each port.

Modem Pass through

The OneOS-based voice-capable router can switch to a G.711 coding mode dynamically during a voice communication when a modem or Super Group 3 FAX is detected. The echo-cancellation is automatically disabled. Several methods are proposed to force the communication to G.711:

- Direct mode: proprietary method consisting in switching the RTP flow to G.711 without notifying the call agent.
- The OneOS-based voice-capable router indicates the Call Agent that a modem tone is detected (the Echo Canceller is disabled). The Call Agent switches the coding mode to G.711 by modifying the connection.

11.1.3.3 DTMF Processing

DTMF can be processed by using the DTMF MGCP package. The DTMF codes are detected in the received voice signal, suppressed before sending the RTP flow and regenerated at the remote end. The DTMF level and duration are configurable.

The DTMF can also be transported transparently in the RTP flow by using the RFC2833 (or directly in case of G.711); in that case, the voice frames are replaced by special RTP frames containing only information about the DTMF code. This is the recommended method.

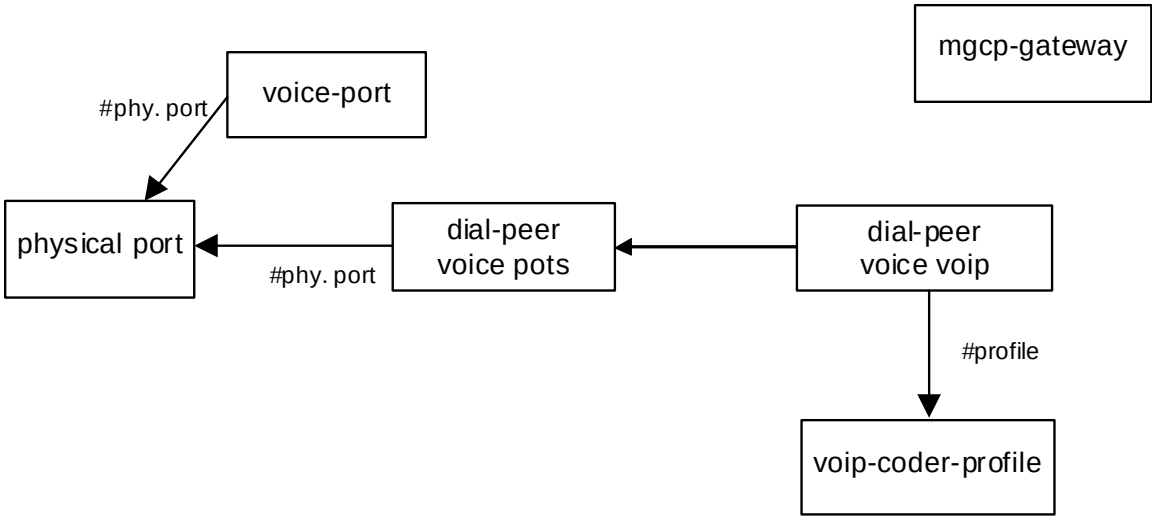
11.2 MGCP CONFIGURATION

11.2.1 Introduction

A set of command lines (CLI) enables the configuration of all necessary parameters. The configuration includes the following main commands:

- Voice-port: Physical FXS port. Voice processing parameters are defined such as echo cancellation, gain and coding law.
- Dial-peer voice: Logical internal ports.
- Pots: Local voice port always associated with a physical port. It enables the configuration of groups, direct call and number transformation.
- VoIP: MGCP endpoint. The coder profile and how to process DTMF and FAX/Modem are defined here.
- VoIP-coder-profile: to define a list of coders to be negotiated during capabilities exchange.
- MGCP-gateway: defines all the parameters related to the MGCP protocol (Call Agent, gateway identifier).

The relationships between configuration items are described in the following diagram:



The following sequence for configuration is preferred:

1. voice ports
2. dial-peer voice POTS
3. voip coder profiles
4. dial-peer VoIP
5. MGCP gateway

11.2.2 Configuration

All the parameters enter in effect immediately, except a few parameters specified in MGCP-gateway. For these parameters, a shutdown command of the MGCP-gateway is required (this requirement is indicated by a Warning message).

11.2.3 Physical Voice Ports

The OneOS-based voice-capable router voice module is always designated by the number 5. On a FXS module, the physical port is identified with a port number in the [0..(n-1)] range, where n is the total port number of the interface module (currently up to 13).

Command for creation of physical port #0 (voice module #5):

```
CLI(configure)> voice-port 5/0
```

11.2.3.1 Parameters for Echo Cancellation

Use the following command to enable the echo canceller – default: enable. Use the `no` form to disable echo cancellation.

```
CLI(voice-port)> [no] echo-cancellation
```

Use the following command to define the maximum tail length; `low` is 8ms, `medium` is 16ms, `high` is 32 ms. It must be configured `medium` or `high` if off-net calls must be supported (default value: `medium`).

```
CLI(voice-port)> echo-cancellation-length { low | medium | high }
```

On ONE300, when using G.729 codec, 30 voice channels can only be supported if echo-cancellation low or medium is selected.

To specify the conditions for automatically disabling the echo canceller on FAX or modem detection, use the following command. Default: no echo disabling. See the table on page 6.2-37 for the explanation of the parameter.

```
CLI(voice-port)> echo-disable { voicemodem | modem }
```

11.2.3.2 Parameters for Gain control

Use the following command to set the output gain (dB) that amplifies the signal for the voice flow sent to the remote VoIP peer – default: 0 (no gain).

```
CLI(voice-port)> output-gain <gain>
```

Use the following command to set the input gain (dB) that amplifies the signal for the voice flow received from the remote VoIP peer – default: 0 (no gain).

```
CLI(voice-port)> input-gain <gain>
```

11.2.3.3 Parameters for Ringing

For analog ports only, use the following command to specify the ring signal parameters. The frequency used is compliant to these country specifications. Default: France.

```
CLI(voice-port)> ring { Australia | Austria | Belgium | Denmark | France
                      | Germany | Ireland | IrelandUK | Italy
                      | Netherlands | Portugal | Spain | Sweden
                      | Switzerland | UK | USA | userdefined }
```

Use the following command to define the ringing parameters for the `userdefined` ringing profile. `Freq` is the frequency from 0 to 60 Hz, `ton` / `toff` are the emission/pause durations in ms (0-5000).

```
CLI(voice-port)> user-ring <freq> <ton-1> <toff-1> <ton-2> <toff-2>
```

Use the following command to specify the standard to be applied.

```
CLI(voice-port)> caller-id { none | dtmf | fsk }
```

Use the following command to specify the initial ring tone (ms) for caller-id.

```
CLI(voice-port)> initial-ring <10-2000>
```

Use the following command to define the ringing voltage, for analog ports only, (default: normal).

```
CLI(voice-port)> ring-level { normal | high | max }
```

See 6.2.3.1 for more information about the available ring levels.

11.2.3.4 Parameters for Tones

Use the following command to specify the tones signal parameters. The frequencies and durations used comply with the selected country specifications.

```
CLI(voice-port)> tone { Australia | Austria | Belgium | Denmark | France
                      | Germany | Ireland | IrelandUK | Italy
                      | Netherlands | Portugal | Spain | Sweden
                      | Switzerland | UK | USA }
```

Use the following command to specify the transmit level for tones (dBm). Default: -10 dBm.

```
CLI(voice-port)> tone-level <-40 to 0>
```

The following command can be used, after having selected a country, to modify the characteristics of one or more tones if needed.

```
CLI(voice-port)> modify-tone { dial | network-failure | congestion | busy
                             | ring-back | mwi | call-waiting | other
                             | specific-info | specific-conf }
                             <new-tone-specs-string>
```

For any tone command received from the remote Call-Agent and not referenced as a dedicated tone, the `other` tone is used (whose default format is the busy tone format).

Refer to 6.2.1.4 for a complete description of the `new-tone-specs-string` parameter.

The following commands are deprecated and replaced by the above defined command.

```
CLI(voice-port)> tone userdefined
CLI(voice-port)> user-tone …
CLI(user-tone)> timing …
CLI(user-tone)> frequency …
```

11.2.3.5 Parameters for Dialing

Use the following command to define the transmit level for DTMF digits (dBm). Default: -12 dBm.

```
CLI(voice-port)> digit-level <-32 to 0 dBm>
```

Use the following command to define the transmitted DTMF digit duration. Default: 100ms.

```
CLI(voice-port)> digit-duration <50 to 1000 ms>
```

Use the following command to define the minimum delay between two DTMF digits (for transmission towards the terminal). Default: 100ms.

```
CLI(voice-port)> inter-digit <50 to 1000 ms>
```

11.2.4 Internal Local Voice Port (POTS)

The command for the creation of a local POTS port associated with the 5/port physical port is:

```
CLI(configure)> dial-peer voice pots <n>
CLI(pots)> port 5/<port>
CLI(pots)> exit
```

Each dial-peer voice pots must be identified by an arbitrary index n from 0 to N. The physical port numbering is defined in the product installation manual.

11.2.5 MGCP Gateway

This command defines the global parameters for the H.323 gateway:

```
CLI(configure)> mgcp-gateway
CLI(mgcpgw)>
```

11.2.5.1 Parameters

Use the following command to shutdown the MGCP gateway. Changes on parameters concerning the MGCP gateway are effective after a shutdown/no shutdown operation. Default: shutdown. Enter the no shutdown command when you have completed the configuration of the MGCP gateway parameters.

```
CLI(mgcpgw)> [no] shutdown
```

Use the following command to define the IP interface attached to the MGCP gateway (may be Ethernet, FastEthernet, ATM, PPP ...) that serves as source IP address of the gateway. The IP address of the MGCP gateway is the IP address configured for this interface (or dynamically acquired in case of PPP/IP-CP).

```
CLI(mgcpgw)> gw-interface <IP interface>
```

Use the following command to configure the call agent IP address and UDP port. The UDP port is optional (default: 2727).

```
CLI(mgcpgw)> call-agent-add <IP-address>[:<port>]
```

Use the following command to define the gateway identifier for the call agent (mandatory). identifier is a string of 40 characters maxi.

```
CLI(mgcpgw)> gw-id <identifier>
```

Use the following command to define the UDP port range used for RTP (each 0-65535). Default 16384-16482.

```
CLI(mgcpgw)> rtp-port-range <0-65535> <0-65535>
```

Use the following command to send RSIP packets periodically to keep NAT sessions open on the path to the call agent (not active by default).

```
CLI(mgcpgw)> [no] keep-alive
```

Use the following command to specify the time interval to use for the MGCP keepalive timer if option keepalive is set. Default value is 30 sec.

```
CLI(mgcpgw)> keep-alive-timer <10..600 seconds>
```

Example:

```
CLI(configure)> mgcp-gateway
CLI(mgcpgw)> gw-interface ATM 0.1
CLI(mgcpgw)> call-agent-add 10.2.2.1
CLI(mgcpgw)> rtp-port-range 32000 36000
CLI(mgcpgw)> no shutdown
```

11.2.6 VoIP Coder Profiles

It is possible to define a list of coders for the terminal capabilities. The list contains the preference order, in which the codec shall be used when negotiating the codec with the remote VoIP endpoint.

Commands:

```
CLI(configure)> voip-coder-profile 1
CLI(voip-coder)> codec 1 g711 20
```

```
CLI(voip-coder)> codec 2 g729ab 10
```

Parameters:

```
CLI(voip-coder)> codec <preference-index> <codec> [<sample-time-length>]
```

- `preference index`: indicate the position in the list of coders (1 to 10).
- `codec`: may be g729ab, g711a, g711u.
- `sample-time-length`: period of frames transmission (in ms). Allowed values are:
  - `g729ab`: 10, 20, 30, 40. Default: 20.
  - `g711a, g711u`: 10, 20, 30, 40. Default: 20.

The selected coder will be the first one in the list matching with the remote capabilities.

11.2.7 Voice over IP Dial Peer

The VoIP port is defined as a 'Voice over IP Dial Peer', that identifies an MGCP endpoint.

To create a dial-peer VoIP, enter:

```
CLI(configure)> dial-peer voice voip <index>
```

One can create several VoIP dial peers; therefore, an arbitrary number identifies each dial peer.

11.2.7.1 Parameters

Use the following command to define the protocol used for this dial-peer. It must be set to “MGCP” (the default value is h323).

```
CLI(voip)> sig-protocol mgcp
```

Use the following command to define the local port bound to this MGCP endpoint (dial-peer port).

```
CLI(voip)> mgcp-dppots <dial-peer pots identifier>
```

Use the following command to define the name of the endpoint. The recommended value is "`aaln/x`" where x is the port number.

```
CLI(voip)> mgcp-ep <endpoint name>
```

Use the following command to define the coder profile to use. Default: 0. If the coder profile is not defined, the G.711A/20ms coding mode is used.

```
CLI(voip)> voip-coder-profile <0-9>
```

Use the following command to enable the silence detection and suppression. The value `vadcng` can be used for G.711 and G.726 to enable the comfort noise generation (this feature is de-facto enabled if `vad` is configured with G729AB and G723.1). Use the `no` form to disable the voice activity detection. Default: disable.

```
CLI(voip)> silence-detection { vad | vadcng }
```

Use the following command to specify the DTMF management mode. If 'out-of-band' is selected, DTMF are sent using DTMF MGCP package. If in-band is selected, the DTMF are transmitted in RTP frames (cf. RFC 2833). Default: none.

```
CLI(voip)> dtmf-relay { none | in-band | out-of-band }
```

Use the following command to specify the fax management. Default: none. It specifies the fax management. Default: none. `passthrough` is configured for an automatic codec switching to G.711. The method is configured by the command `passthrough-mode`.

```
CLI(voip)> fax-relay { none | passthrough | T38 }
```

Use the following command to define the number of T.38 frames for redundancy. Default: 0.

```
CLI(voip)> t38-redundancy <0-4>
```

Note that adding frames for redundancy can increase a lot (up to 5 times) the needed bitrate, especially for high rate modulations. Provision has been taken to avoid such drawback, refer to the table on page 6.9-81.

The T.38 fax relay is supported in strict or loose mode. The strict mode requires the remote gateway to explicitly indicate T.38 support, so that a T.38 fax relay communication can start. Refer to RFC 5347 for more information.

```
CLI(voip)> mgcp-t38-mode { none | loose | strict }
```

Use the following command to enable the automatic modem detection. Default: no. The method used for up-speed is defined by the command passthrough-mode.

```
CLI(voip)> modem-passthrough
```

Use the following command to define the jitter max value. Default: 100ms. The jitter compensation buffer is initialized such that it is half-way filled. When the jitter compensation buffer is filled above this limit, an excessive jitter event is raised indicating that the voice flow encounters severe jitter.

```
CLI(voip)> jitter <20..1000 ms>
```

11.3 MGCP CONFIGURATION EXAMPLE

To use these configuration examples, copy & paste the following command lists in a configuration file or to the CLI.

Configuration environment: 4 FXS ports

```
! Physical voice ports declaration
voice-port 5/0
exit
voice-port 5/1
exit
voice-port 5/2
exit
voice-port 5/3
exit

! local voice ports

dial-peer voice pots 0
port 5/0
exit
dial-peer voice pots 1
port 5/1
exit
dial-peer voice pots 2
port 5/2
exit
dial-peer voice pots 3
port 5/3
exit


! Voice coder list (terminal capabilities)

voip-coder-profile 1
codec 1 g729ab 20
codec 2 g711a 20
exit

! dial-peer voip : remote voip devices

dial-peer voice voip 0
sig-protocol mgcp
mgcp-dppots 0
mgcp-ep aaln/1
voip-coder-profile 1
exit

dial-peer voice voip 1
sig-protocol mgcp
mgcp-dppots 1
mgcp-ep aaln/2
voip-coder-profile 1
exit

dial-peer voice voip 2
sig-protocol mgcp
mgcp-dppots 2
mgcp-ep aaln/3
voip-coder-profile 1
exit
```

```
dial-peer voice voip 3
sig-protocol mgcp
mgcp-dppots 3
mgcp-ep aaln/4
voip-coder-profile 1
exit


! MGCP gateway global parameters (gatekeeper)

mgcp-gateway
gw-interface fastethernet 0
call-agent-add 200.15.0.103
gw-id oneaccess.com
no shutdown
exit
```

11.4 MGCP STATISTICS DISPLAY

The Command Line Interface provides access to statistics and configuration status for the voice service. The 'show' commands can be used at any level in the CLI tree.

The syntax is the following:

```
CLI> show voice <parameters> <index>
```

With:

`parameters`: Defines the port or the connection.

`index`: Specifies the port or connection number. `all` specifies all ports or connection.

11.4.1 FXS Voice Port Statistics

To show statistics on a FXS physical port, enter:

```
CLI> show voice voice-port fxs index 0
        voice port                              5/2
                current state                   on hook
                config state                    up
                attached mgcp dial peer         0
                voice communication             no

                Outgoing calls                          0
                Outgoing calls failures                 0
                        Unsufficient pots-group resource        0
                                User busy (17)                  0
                                No answer (18)                  0

                Incoming calls                          0
                Incoming calls backup invoked           0
                Incoming calls failures                 0
                        Remote failure                          0
                        Unknown number                          0
                        DSP unavailable                         0
                        No VoIP ressource available             0
                        Not specified                           0
```

Note:

- Outgoing call statistics are related to the calls towards the FXS device or network (transmitted by the OneOS-based voice-capable router on this port).
- Incoming call statistics are related to the calls coming from the FXS device or network (received by the OneOS-based voice-capable router on this port). "Remote failure" indicates that the failure has occurred on the outbound port (VoIP or local).
- Voice communication is indicated as "yes" if a communication is in progress.
- `show voice voice-port fxs all` displays statistics on all the voice ports.

11.4.2 Dial Peer VoIP Statistics

To show statistics for the dial-peer VoIP `<port-id>`, use the following command:

```
CLI> show voice dial-peer voice voip index <port-id> [<type>] [reset]
```

To show statistics for all the dial-peer VoIP, use the following command:

```
CLI> show voice dial-peer voice voip all [<type>] [reset]
```

type may be:

- current: statistics on current calls.
- outgoing: statistics on outgoing calls only.
- incoming: statistics on incoming calls only.
- user-plan: statistics on voice & fax only.
- all (default): all the statistics are provided.

```
CLI> show voice dial-peer voice voip index 0
Dial Peer                                                   1
 Current protocol                          h323
 Current Calls                                              1
                          Outgoing Calls
         Outgoing Calls                    221
         Outgoing calls failures           14
         RAS Call Failures                           0
                 Admission time-out                         0
                 Admission Rejects                          0
         H225/Q931 Call failures                     14
                 Cause Class 0 (normal event)               0
                 Cause Class 1 (normal event)               4
                         Normal Cause (16)                  0
                         User busy (17)                     0
                         No answer (18)                     0
                 Cause Class 2 (unavailable ressources)     10
                 Cause Class 3 (unavailable service)        0
                 Cause Class 4 (service not provided)       0
                 Cause Class 5 (invalid message)            0
                 Cause Class 6 (protocol error)             0
                 Cause Class 7 (interworking)               0
                H245 Call failures                         0
                 Incompatible capabilities                  0
                 Protocol errors                            0
         Internal call failures                      0
                 DSP unavailable                            0
                 Max-bandwidth exceeded                     0
                 Max-connection exceeded                    0
                 Gateway not registered                     0
                 Gateway status down                        0
                 Not specified                              0
                         Incoming Calls
         Incoming calls                    345
         Incoming calls failures           14
         RAS Call failures                           0
                 Gatekeeper Unavailable                     0
                 Admission Rejects                          0
         Local Port Call failures                    0
         H245 Call failures                          0
                 Incompatible capabilities                  0
                 Protocol errors                            0
         Internal call failures                      14
                 DSP unavailable                            0
                 Unknown number                             0
                 Channel / port unavailable                 0
                 Max-bandwidth exceeded                     0
                 Max-connection exceeded                    0
                 Not specified                              14
         Advice-of-charge                            0
                          Voice & Fax statistics
 RTP statistics
         Number of transmitted packets                      35
```

```
        Number of received packets                      40
        Number of transmitted bytes                     11620
        Number of received bytes                        13280
        Number of excessive jitter events               0
        Number of lost packets                          0
        Number of invalid packets                       0
Number of calls with frame error rate
         total <0.01%  <0.1%  <0.5%    <1%    <5%   >=5%
           565    565      0      0      0      0      0
Modem passthrough
        Number of switching to modem mode               0
T38 FAX Calls
        Number of outgoing fax                          0
        Number of incoming fax                          0
        Number of failures                              0
                Request Mode failure                    0
                Pre-message procedure failure           0
                Page failure                            0
        Number of transmitted packets                   0
        Number of received packets                      0
        Number of transmitted bytes                     0
        Number of received bytes                        0
        Number of lost packets                          0
```

Note:

- Outgoing call statistics are related to the calls towards the H.323/SIP network (transmitted by the OneOS-based voice-capable router to the remote VoIP device.
- Incoming call statistics are related to the calls coming from the H.323/SIP network (received by the OneOS-based voice-capable router from a VoIP device). "Remote failure" indicates that the failure has occurred on the outbound port (local).

11.4.3 MOS Scoring Statistics

The following command gives statistics about the voice quality:

```
CLI> show voice mos

------------------------ Call Quality ------------------------

    Number of Call       : 10
    Average of MOS       : 3.58
    Minimum MOS          : 2.38
    Maximum MOS          : 4.29
    Average of ERL       : 41
    Average of ACOM      : 67
    Average of loss-rate : 0
    Average of jitter    : 14
    Average of Max delay : 16
--------------------------------------------------------------
```

Use the following command to reset and restart the MOS scoring statistics:

```
CLI> show voice mos reset
```

11.4.4 MGCP Gateway Statistics

The following command gives statistics about the gatekeeper:

```
CLI> show voice mgcp-gateway

Call Agent IP address        200.105.0.103:2427
Connection state             connected
 Current Calls                                      0
                      Outgoing Calls
```

```
            Outgoing Calls                                  0
            Outgoing calls path established                 0
                              Incoming Calls
            Incoming Calls                                  0
            Incoming calls path established                 0
```

Note:

- Outgoing call statistics are related to the calls coming from the analog phone
- Incoming call statistics are related to the calls sent to the analog phone
- Voice communication is indicated as "yes" if a path is established
- The connection state is “connected” when the RSIP message is acknowledged

11.4.5 Events

- `FXS port <5/x> event {off-hook | on-hook | ringing on | ringing off}, pots = <dp pots>`: event on FXS analog port.
- `Digit <x> received, pots = <dp pots>`: digit reception (dialing).
- `MGCP Call Agent connection`: connected to the call agent (RSIP acknowledged).
- `MGCP Call Agent connection failure`: connection error.
- `Voice port <5/x> status change: {shutdown | no shutdown}`: indicates that the interface has been shutdown by the operator. The port cannot be used for calls.
- `MGCP RTP transmission {started | stopped}, dp-voip = <dp voip>, coder <coder>`: indicates that the OneOS-based router has started (or stopped) to send RTP packets.
- `MGCP RTP reception {started | stopped}, dp-voip = <dp voip>, coder <coder>`: indicates that the OneOS-based router is able (or not able) to receive RTP packets.
- `MGCP FAX T38 starting, dp-voip = <dp voip>`: start of the T38 call.
- `MGCP FAX T38 end of call, dp-voi p = <dp voip>`: end of the T38 call.
- `MGCP FAX T38 call failure, dp-voip = <dp voip>, cause <T38-cause>`: indicates the T38 cause.
- `MGCP FAX T38 Pre-message procedure OK, dp-voip = <dp voip>`: indicates that the T38 call is connected.
- `MGCP FAX T38 {receiving | transmitting} page <n>, dp-voip=<dp voip>`: indicates that the page n is being received / transmitted.
- `MGCP FAX T38 page <n> {OK | KO}, dp-voip = <dp voip>`: indicates that the page n has been received / transmitted OK or not.
- `MGCP FAX T38 <n> IFP packets lost, dp-voip = <dp voip>`: indicates a T38 transmission error.
- `MGCP FAX/Modem start of detection, dp-voip = <dp voip>`: indicates that a fax or modem call is being detected.
- `MGCP FAX/Modem end of detection, dp-voip = <dp voip>`: indicates that the detection phase has ended.
- `DSP failure <dsp number> <failure nb>`: indicates a DSP internal error (software crash).
- `MGCP <number> invalid voice packets received, dp-voip = <dp voip>`: number of invalid voice packets received.
- `MGCP <number> voice packets lost, dp-voip = <dp voip>`: number of voice packets lost.
- `MGCP <number> excessive jitter, dp-voip = <dp voip>`: the jitter is greater than the configured threshold value.

11.5 MGCP TROUBLESHOOTING TOOLS

Events and statistics described above should be used first for troubleshooting call failure. This section describes other useful tools.

11.5.1 LEDs

The voice service is fully operational if all these conditions are OK:

- The IP interface attached to the MGCP gateway is UP.
- The connection with the Call Agent is established.

11.5.1.1 ONE200/400 (two "Voice" LEDs)

Led **Voice**:

- Green: Voice service fully operational.
- Red: Voice service configured but not fully operational.
- Off: The voice service is not configured.

Led **Com**:

- Green: At least one voice communication (path) is established.
- Off: No voice communication in progress.

11.5.1.2 Other ONEXX0 devices (only one "Voice" LED)

Led **Com**:

- Green: Voice service fully operational, no call in progress.
- Blinking green: Voice service fully operational, call in progress.
- Red: Voice service configured but not fully operational.
- Off: The voice service is not configured.

11.5.2 MGCP protocol capture

It is possible to display on the console port or on a Telnet client the packets which are exchanged between the MGCP gateway and the call agent.

To display the packets:

```
CLI> [no] debug mgcp
```

11.5.3 RTP Call Detailed Reports

The RTP session monitoring feature gives history information about jitter and packet loss. The last 200 calls and the current calls are monitored.

To display the statistics:

```
CLI> show voice rtpcall { short | full } { any | err }
                              { all | min <val1> max <val2> | ind <value> }
```

Two modes are available:

- `short`: statistics summary

- `full`: all the statistics

A filter can be applied to get only the calls with errors: `any` or `err`

The calls are numbered as following: the 1st is the most recent one and the last call is the oldest one. The first calls can be in progress or not.

Several options are available to select the calls:

- `all`: all the calls from 1 to 100
- `min <value1> max <value2>`: all the calls between value1 and value2
- `ind <value>`: the call specified by the value

Example:

```
CLI> show voice rtpcall short any min 1 max 3

  1 - 01/04/01 00h47m43s RTP 20.5.3.131:16418 - 200.15.0.152:16390
      Play time (voice) : 00h00m47s
      RTP Packets RX / TX : 2338 / 2337
      RTP Packet lost&discarded RX / TX (RTCP reported) : 0 / 0
      Number of Excessive Jitter events : 1
      Max Interarrival jitter (uplink) Rx / Tx: 9 ms / 1 ms

  2 - 01/04/01 00h47m24s RTP 20.5.3.131:16416 - 200.15.0.152:16388
      Play time (voice) : 00h00m46s
      RTP Packets RX / TX : 2337 / 2338
      RTP Packet lost&discarded RX / TX (RTCP reported) : 0 / 0
      Number of Excessive Jitter events : 1
      Max Interarrival jitter (uplink) Rx / Tx: 9 ms / 1 ms

  3 - 01/04/01 00h47m05s RTP 20.5.3.131:16414 - 200.15.0.152:16476
      Play time (voice) : 00h00m47s
      RTP Packets RX / TX : 2332 / 2331
      RTP Packet lost&discarded RX / TX (RTCP reported) : 0 / 0
      Number of Excessive Jitter events : 1
      Max Interarrival jitter (uplink) Rx / Tx: 9 ms / 1 ms
```

In full mode:

```
CLI> show voice rtpcall full any ind 2

  2 - 01/04/01 00h47m24s RTP 20.5.3.131:16416 - 200.15.0.152:16388
      Play time (voice) : 00h00m46s
      Tx Coder : G729 / 20 ms ; Rx Coder : G729
      VAD enabled local / remote : no / no

      ERL   : -- dB
      ACOM  : -- dB

      RTP Packets received (DSP / Uplink) : 2337 / 2337
           lost : 0
           out of sequence : 0
           invalid : 0
      RTP Packets transmitted (DSP / Uplink) : 2338 / 2338
           lost (RTCP reported) : 0

      Jitter parameter : 100 ms
      Number of Excessive Jitter events : 1

      Excessive Jitter events :
 2|
 1|  *
  ----------------------------------------
      0  30"   1'   2'   4'   8'  12' >16'


Press any key to continue (Q to quit)
```

```
     Jitter received (uplink) :
          Max delay : 93 ms
          Delays (ms)     >50  >100  >150  >200  >300
          Nb of occur.      2     0     0     0     0
          Interarrival max jitter : 9 ms
     Jitter received (DSP) :
          Max delay : 93 ms
          Delays (ms)     >50  >100  >150  >200  >300
          Nb of occur.      2     0     0     0     0
          Interarrival max jitter : 9 ms

     Frames with a delay >50 ms :
2|
1|  *    *
 ----------------------------------------
     0  30"   1'   2'   4'   8'  12' >16'

     Jitter transmitted (uplink) :
          Max delay : 6 ms
          Delays (ms)     >50  >100  >150  >200  >300
          Nb of occur.      0     0     0     0     0
          Interarrival max jitter : 1 ms
                  (RTCP reported) : 2 ms
```

Notes:

- ERL is the Echo Return Loss measured before echo cancellation. ACOM is the echo return loss measured after echo cancellation.
- When a value has not been calculated, it is replaced by a "-". Examples: uplink analysis is disabled, the ERL & ACOM when an echo situation has not been encountered (an echo situation is a high transmitted audio signal and low received audio signal), no RTCP packets received.
- A graph indicates the time distribution of the errors. The 30 sec column indicates the number of errors occurred between 30 sec and 1 min after the beginning of the call.
- For the jitter statistics, "delay" means the time between two packets decreased by the normal time. Example: a delay of 80ms for a 20ms coder sample length causes a jitter of 60ms towards expected value.
- The inter-arrival jitter is calculated for each packet in conformance with the RFC3550. The indicated value is the max jitter observed during the call.

12 RTP CLOCK SYNCHRONIZATION

12.1 RTP CLOCK SYNCH OVERVIEW

The RTP clock synchronization solution is designed to synchronize real-time clocks in the nodes of a distributed system communicating over an IP packet network. The clock synchronization mechanism overcomes the asynchronous nature of packet switched networks and regenerates a reference clock accurately across the IP network.

Packet arrival at a particular network node is typically characterized by slow and smooth drifting of packet arrival rate referred to as wander (mimicking the original transmission clock drift) and fast random jumps caused by processing delays (caused by routing and switching nodes, packet bursts, congestion, overload or topology changes) that are called jitter. The RTP clock synchronization solution makes it possible to recover a reliable clock from a stream affected by jitter. Namely:

Quickly derive the reference clock from the packet stream,

Lock onto the reference clock and regenerate a clean clock signal,

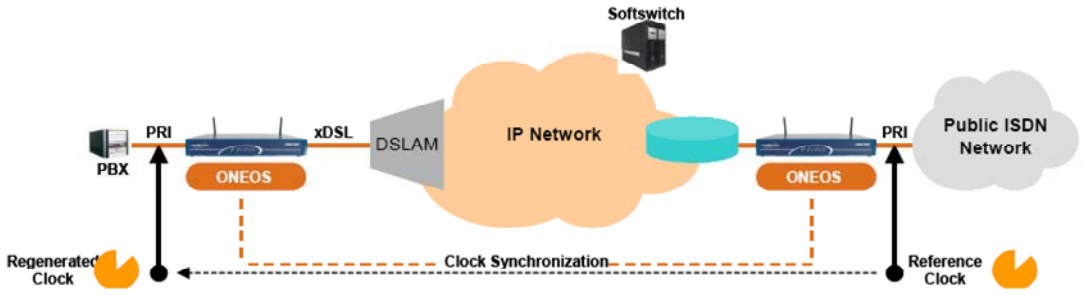
Adapt the system clock to track the reference clock and maintain long-term accuracy.

12.2 RTP CLOCK SYNCH DESCRIPTION

The OneAccess solution is based on two or more OneOS peers. One peer extracts the reference clock from a reference interface (such as PRI connected to the public network) and transmits it over the packet switched network. The remote peer(s) regenerate(s) the clock rate distributed by the originating node. The synchronization solution is four-fold:

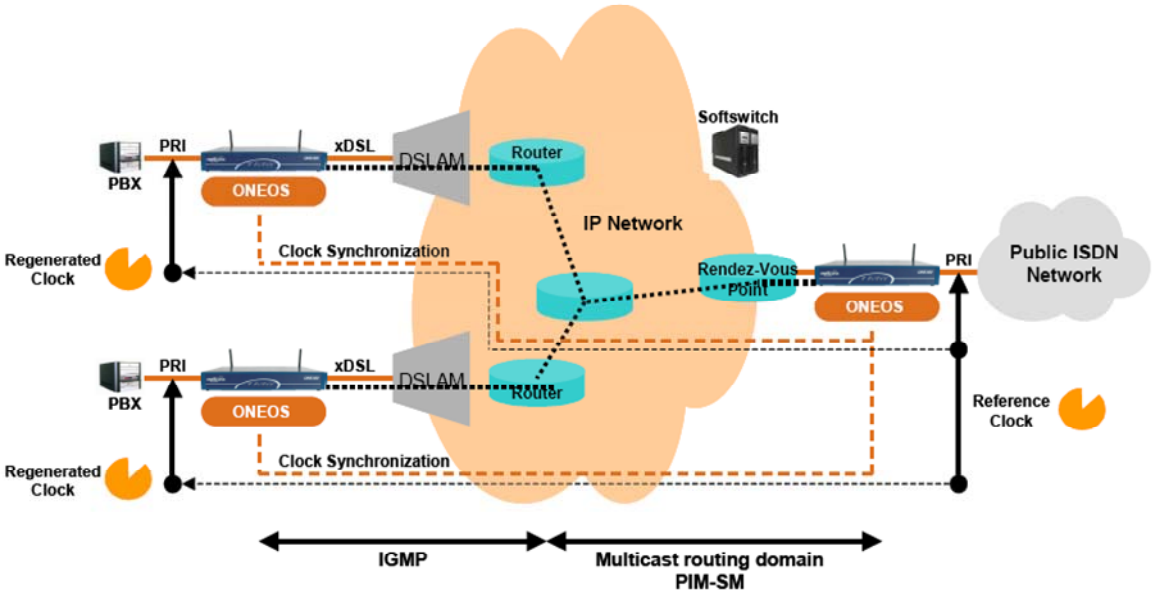
1. It captures the reference clock rate from which other nodes in the network derive their own clock thus establishing a hierarchy of time synchronization. The reference clock is derived from an extremely accurate clock on a T2 or T0 interface or via the xDSL uplink that usually delivers the ATM network physical layer clock reference.
2. The packet switched data network does not inherently deliver any clocking information to network nodes therefore the OneAccess solution uses out of band packets to transfer the clock information to other network nodes. It transmits the original clock via RTP packets sent at a specific stream rate.
3. The distribution of the reference clock information over the packet switched network exploits the routing capabilities of IP networks and offers two options:

    - Point-to-point clock distribution to synchronize a reference clock with one or several pre-configured remote peers:



Typical point to point clock synchronization application

- Point-to-multipoint clock distribution by means of multicast routing protocols:

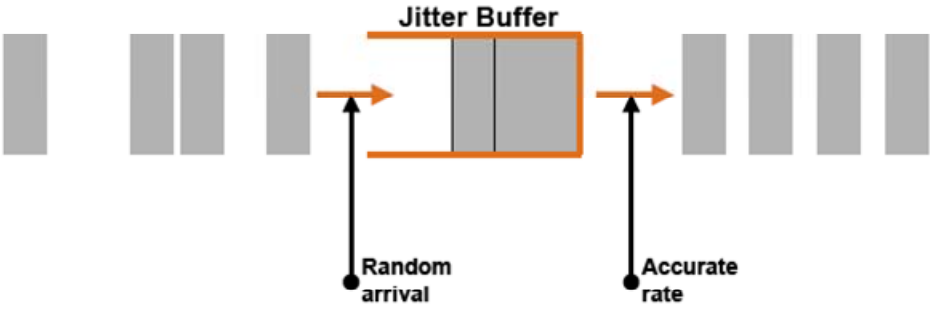


Typical point to multi-point clock synchronization application

4. The receiving node processes the synchronization packets with a kind of averaging process that annihilates the effect of jitter and captures the reference clock rate. It then regenerates a clean clock signal derived from the reference clock. The algorithm also detects changes happening in the network and adapt to these variations in order to track specifically the reference clock.

12.3 RTP CLOCK SYNCH ALGORITHM

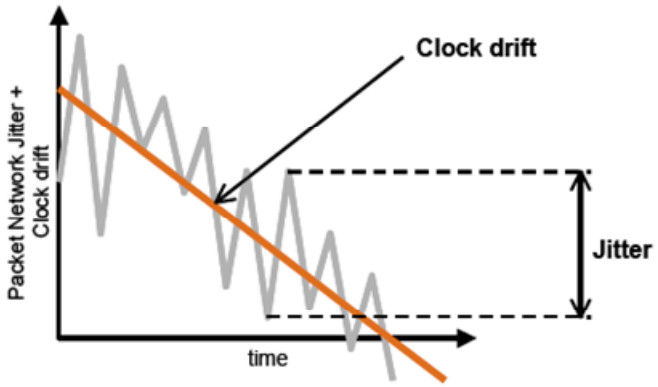
The regeneration of the reference clock is based on a jitter buffer that absorbs the network delay fluctuations and clocks out the incoming data at a precise rate locked on the reference clock.



Jitter Buffer Principle

The device internal oscillator is driven by the clock synchronization algorithm such that buffered data are read out at a constant rate matching the reference clock rate. The continuous adjustment of the buffer output rate to the reference clock is called adaptive clocking.

The RTP stream is dedicated to adaptive clock recovery. It is combined with advanced algorithms allowing OneOS to filter out the network transmission delay and calculate over time the variation of the network jitter together with the difference in packet time transmission introduced by the clock drift between the reference clock and the device internal clock as pictured below.



Network Jitter and clock drift measurement

These calculations are used to determine the clocking difference between the device's clock and the reference clock represented by the slope of the linear interpolation of the jitter + clock drift curve. The correction factor value to be applied to the device oscillator directly flows from this slope and allows OneOS to synchronize the buffer clock rate to the reference clock rate. The slope represents the direction and magnitude of the clock difference between the two ends of the network.

The OneOS clock synchronization algorithm is designed to ensure:

- Fast convergence of the devices' clock toward the reference clock.
- Complete filtering of the network jitter and packet delay variation to recover the exact reference clock.
- Track short-term deviations of the reference clock to guarantee data integrity for upper layer applications.

These seemingly contradictory goals are achieved with a multistage algorithm as illustrated below.

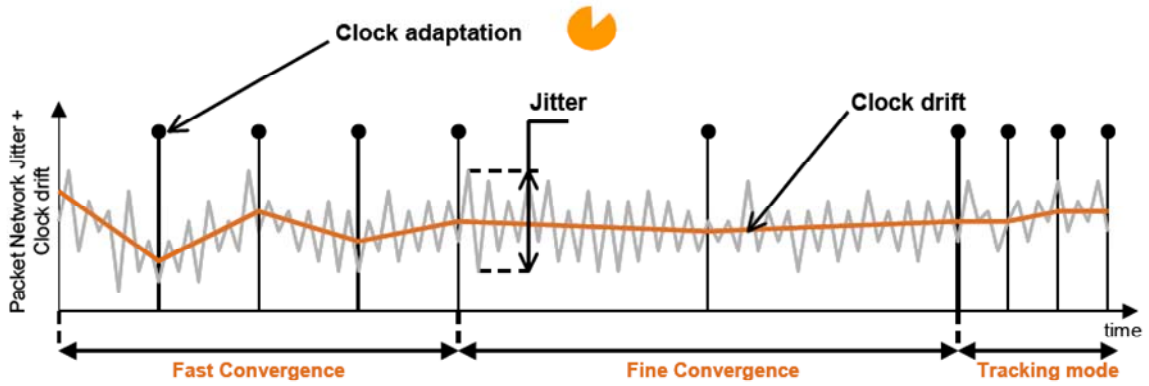
In a first phase called **Fast Convergence** (phase #1) the algorithm makes coarse adjustments of the clock rate to rapidly converge toward a good approximation of the reference clock. Clock adjustments conclude observation periods during which OneOS monitors the jitter and clock drift variations. A slight or null slope indicates that the clock difference between the two ends of the network is almost zero.

Observing the difference between the device's clock and the reference clock for some time can be seen as a kind of averaging process that filters the effects of the random network variations to capture the original clock rate.

At the end of the Fast Convergence phase OneOS already has synchronized the clock to a decent estimate of the reference clock and enters into the **Fine Convergence** (phase #2) mode. The fine convergence mode defines longer monitoring periods allowing OneOS to filter out the random delay variations introduced by the network. Fine clock rate adjustments are driven by slope calculations during these periods. Any frequency discrepancy between the reference and device's clocks is eventually compensated, and the OneOS precisely aligns the two clock frequencies.

Finally, when the clock difference has gotten small enough, OneOS enters in the **Tracking Mode** (phase #3) which is designed to optimize clock adjustments so that the regenerated clock follows oscillations of the reference clock. In this phase OneOS uses much smaller clock adjustments but the frequency of the adjustments is increased to better track the reference clock variations and avoid late corrections of the clock rate.

The algorithm includes defense mechanisms that allow OneOS to downgrade the synchronization process from one mode to another in order to ensure fast clocking convergence even in adverse network conditions (network outages, packet loss, congestion…).



Clock Synchronization process

The process used by OneOS to mimic the reference clock rate is actually more sophisticated than that described above. Complex digital signal processing techniques are applied to determine the best clock correction values and the optimum threshold values allowing moving from one stage to another.

12.4 RTP CLOCK SYNCH CONFIGURATION

12.4.1 Voice ports

To enable the RTP clock synchronization, the following command must be entered in the voice-port parameter group:

```
CLI(configure)> voice-port 5/0
CLI(voice-port)> clock-source rtp
CLI(voice-port)> exit
```

12.4.2 Peer-to-Peer Mode

This mode is configured on the client device only: the internal call generator is used to call a remote device which is synchronized on the reference clock. The remote device may be an OneAccess gateway with the automatic internal responder.

To enable the RTP synchronization, the internal call generator must use a dial-peer pots with a specific service enabled:

```
CLI(configure)> dial-peer voice pots <n>
CLI(pots)> service clock-recovery
CLI(pots)> exit
```

Note: the "start auto" command must be entered in the VoIP call generator, to have the clock synchronization achieved after a power on.

12.4.3 Multicast mode

For this mode, a specific parameter group is defined:

```
CLI(configure)> voice-global
CLI(voice-global)> [no] rtp-multicast
CLI(rtp-clock)>
```

Use the following command to define the RTP mode:

```
CLI(rtp-clock)> mode { receiver | transmitter }
```

The "transmitter" mode is used on the server side: the device generating the RTP flow synchronized on the reference clock source. The "receiver" mode is used on the client side: the device which get the synchronization from the RTP flow. Default: receiver.

Use the following command to define the IP address of the multicast group.

```
CLI(rtp-clock)> group-address <IP address or hostname>
```

Use the following command to define the IP source address of the RTP flow (used on the transmitter and checked on the receiver side). Default value: empty (no check).

```
CLI(rtp-clock)> source-address <IP address or hostname>
```

Use the following command to define the UDP port to be used. It must be configured to enable the service (no default value).

```
CLI(rtp-clock)> udp-port <port 1-65535>
```

Use the following command to define the payload type to be used in the RTP header. Default: G.711.

```
CLI(rtp-clock)> payload-type <number 0-127>
```

Use the following command to define the time (ms) between two successive RTP packets. Default: 20ms.

```
CLI(rtp-clock)> timestamp <10-20-40>
```

Use the following command to define the time to live (set on the transmitter side). Default: 255.

```
CLI(rtp-clock)> ttl <1-255>
```

Use the following command, only on the transmitter side, to define the IP interface to disable in case of loss of reference clock. It is useful for a backup purpose, with several multicast server devices. Default: disable.

```
CLI(rtp-clock)> [no] sync-interface <ip interface name> <unit>
```

Use the following command to disable or enable the service. The service must be disabled by this command before any parameter value change.

```
CLI(rtp-clock)> [no] shutdown
```

12.5 RTP CLOCK SYNCH STATISTICS

The following command gives some statistics:

```
CLI> show voice clocking
```

Server side

```
RTP clock sender is up and running
  Clock frequency 20 ms
  IP destination address 224.1.1.1:7878, ttl 15
  Source address 192.168.230.2:7878
  Packets sent 5614765, dropped 0
    rate 50 pps (last 4 sec), 50 pps (last min), 50 pps (life avg)
```

Client side

```
RTP clock receiver is up and running
  IP destination address 224.1.1.1:7878
  Source control disabled
  Source 192.168.230.2 since FEB 01 00:04 2000 (1d6h1m)
    packets received 5399711
    rate 50 pps (last 4 sec), 50 pps (last min), 49 pps (life avg)
```

Events are also defined in "`event filter add vox voip userplan gen`" event group to follow any phase change.